UNIVERSIDADE D
COIMBRA

Mariana Oliveira Costa Pereira

PROVA DIGITAL

PROBLEMAS DE COMPATIBILIZAÇÃO ENTRE AS LEIS Nº 32/2008, Nº109/2009 E O CÓDIGO DE PROCESSO PENAL

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses, orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à Faculdade de Direito da Universidade de Coimbra

Maio de 2019

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Mariana Oliveira Costa Pereira

PROVA DIGITAL
PROBLEMAS DE COMPATIBILIZAÇÃO ENTRE AS LEIS Nº 32/2008, Nº109/2009 E O CÓDIGO DE PROCESSO PENAL

Digital Evidence
Problems of compatibilization among the Laws nº32/2008, nº109/2009 and the Code of Criminal Procedure

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2° Ciclo de Estudos em Direito (conducente ao grau de mestre), na Área de Especialização em Ciências Jurídico-Forenses.

Orientadora: Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2019

AGRADECIMENTOS

Primeiramente agradeço à Deus pela oportunidade de estudar e aprender tanto na renomada instituição da Faculdade de Direito da Universidade de Coimbra. Agradeço também à disponibilidade, simpatia e orientação muito enriquecedora da Senhora Doutora Sónia Fidalgo.

Agradeço a minha querida mãe Ana Paula pelo amor, carinho e apoio incondicionais de sempre, bem como minha irmã Milena e meus avós por sempre acreditarem em mim e me motivarem a cada dia ser melhor e nunca desistir de meus objetivos. Agradeço igualmente ao meu querido namorado Mickael pelo seu amor e carinho, por estar ao meu lado em todos os momentos, por me incentivar a realizar meus sonhos, bem como pelas palavras de apoio e motivação. Também não poderia deixar de agradecer as minhas grandes amigas de longa data Marília e Gabriela que apesar do oceano que nos separa estão sempre a mandar energias positivas com seus conselhos, palavras de encorajamento e motivação.

Com certeza não teria chegado até aqui sem o apoio de cada um de vocês e saibam que sou muito grata por tudo que fizeram e fazem por mim.

RESUMO

Tendo em vista os avanços tecnológicos, surgiram crimes informáticos que até então eram impensáveis. Desse modo, foi necessário que as legislações de diversos países se adaptassem à nova realidade através de atualizações, modificações ou com a criação de legislações com o objetivo de combater a cibercriminalidade, meio utilizado principalmente pelo crime organizado e o terrorismo. Nesse sentido, a presente dissertação começa por abordar os principais documentos internacionais que trataram do tema da prova digital, quais sejam a Convenção sobre o Cibercrime do Conselho da Europa de 2001, a Decisão-Quadro nº 2005/222/JAI e a Diretiva nº 2006/24/CE que acabaram por servir de linhas orientadoras para a renovação da legislação portuguesa no que tange a essa matéria. Assim, surgiu a Lei do Cibercrime nº 109/2009 que revogou e substituiu a lei anterior nº 109/91, da criminalidade informática, bem como a Lei nº 32/2008 que veio a regular a conservação e a transmissão de dados de tráfego e de localização, dentre outras. Porém, antes da entrada em vigor dessas leis houve uma reforma do Código de Processo Penal Português em 2007 como tentativa de suprir as lacunas relativas a matéria da prova digital.

Nesse sentido, passa a vigorar a partir de 2009 além de normas gerais sobre a prova digital no Código de Processo Penal, leis especiais sobre a mesma temática. Dessa forma, a presente dissertação veio a tratar dos principais problemas de compatibilização entre esses três diplomas, com o objetivo trazer as melhores soluções que facilitem as investigações e o combate à cibercriminalidade, sem esquecer da proteção dos direitos fundamentais das pessoas que são limitados pelos meios de obtenção e conservação da prova digital, mas que devem ser minimamente afetados.

PALAVRAS-CHAVE

Cibercriminalidade – Prova Digital – Lei do Cibercrime – Problemas de compatibilização – Direitos fundamentais

ABSTRACT

Many cybercrimes that until now were unthinkable appeared due to the technological advancements. In this way, it was necessary to adjust the legislation of many countries to the new reality through updates, changes or through the creation of legislations in order to combat the cyber criminality, which is the main used way by the organized crime and the terrorism. In this way, the following dissertation starts approaching the main international documents that dealt with the subject of digital evidence, which are the Cybercrime Convention of the Council of Europe in 2001, the Framework Decision 2005/222/JAI and the Directive 2006/24/CE that functioned as guidelines to the renovation of the portuguese legislation in this subject. Then the cybercrime law 109/2009 was created which revoked and replaced the previous one, law 109/91 related to the computer crimes, as well as it was created the law 32/2008 which deal with the conservation and transmission of traffic data and location data, among other laws that were created. But before the entry into force of those laws, the Portuguese Code of Criminal Procedure was reformed in 2007 as an attempt of supplying the gaps related to the digital evidence subject.

In this way, since 2009 entered into force general rules about the digital evidence in the Code of Criminal Procedure, besides special laws about that same subject. Then the present dissertation deals with the main compatibilization problems among those three laws with in order to find the best solutions that can make the investigations easier as well as the fight against the cyber criminality without forgetting the people's fundamental rights protection that are limited by the ways of digital evidence's acquisition and conservation but must be minimally affected.

KEYWORDS

Cyber criminality – Digital Evidence – Cybercrime Law – Problems of compatibilization – Fundamental Rights

LISTA DE SIGLAS E ABREVIATURAS

Ac. – Acórdão

Al. – Alínea

Art. – Artigo

Cciber – Convenção sobre Cibercrime do Conselho da Europa

Cfr. – Conforme

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

LCC – Lei do Cibercrime

MP – Ministério Público

Nº - Número

P. – Página

PP. - Páginas

TC – Tribunal Constitucional

TFUE – Tratado de Funcionamento da União Europeia

TJUE – Tribunal de Justiça da União Europeia

TRE – Tribunal da Relação de Évora

TRG – Tribunal da Relação de Guimarães

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

ÍNDICE

I. INTRODUÇÃO

É notório que o desenvolvimento tecnológico[1], com o surgimento da informática, mais especificamente da internet, foi de suma importância e um facilitador de modo geral na vida das pessoas, uma vez que atrás de uma tela e através de um simples "click" compras podem ser feitas, pesquisas, comunicações, transações bancárias, dentre tantas outras atividades, sendo a informática o meio através do qual são possíveis a ocorrência de relações económicas, sociais e culturais[2] à distância. Nesse sentido, percebe-se que é cada vez maior o número de pessoas que têm acesso aos novos meios de comunicação eletrónica em decorrência da diminuição dos seus custos, o que permite que elas possam usufruir das vantagens proporcionadas pela internet.

Porém, assim como a internet traz muitos benefícios, também acaba por servir de meio para o cometimento de diversos crimes, sejam eles informáticos (crimes novos que surgiram em decorrência dos avanços tecnológicos), ou não, no que tange aos crimes já existentes e que podem ser cometidos através da internet. Da mesma forma, o desenvolvimento tecnológico contribui para que os criminosos ocultem[3] suas identidades bem como as provas digitais que levem a sua descoberta, o que acaba por dificultar as investigações, a punição dos culpados e o combate à cibercriminalidade.

Assim, as legislações de diversos países tiveram que se adaptar à nova realidade e passaram a regular os cibercrimes, que até então não existiam, com base em documentos internacionais que se preocuparam em tratar dos problemas decorrentes dos avanços tecnológicos. Juntamente com as normas substantivas foi necessário regular também as

---

[1] "Na contemporaneidade um dos principais fenómenos que se repercute na alteração da sociedade enquanto complexo de comunicações é a evolução tecnológica e a proliferação dos mediadores e dos sistemas de transmissão, captação e registo de som e imagem, com padrões impensáveis há poucos anos em termos de manuseabilidade, fiabilidade, baixo custo, susceptibilidade de manipulação, impressividade", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime", in *Processo Penal, Prova e Sistema Judiciário,* Coimbra Editora, 2010, p. 83.

[2] VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada,* Coimbra Editora, 2011, pp. 14-15.

[3] "(...) aquelas tecnologias permitem a sua utilização à distância, sem qualquer contacto físico com os sistemas informáticos ou dados atingidos. Refere-se que facilitam aos seus utilizadores o encobrimento das respectivas identidades e acções, bastando ter-se presente, por exemplo, que estes podem assumir identidades virtuais, tomar a identidade de terceiros (...), praticar os actos desde um computador ligado à Internet num cibercafé de qualquer parte do mundo ou simplesmente apagar a informação em escassos segundos, carregando numa tecla", MILITÃO, Renato Lopes, "*A propósito da prova digital no processo penal",* 2012, p. 260, disponível em https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf > consultado em 1-04-19;

normas processuais e de cooperação internacional[4] relativas ao tema, uma vez que a recolha e conservação de prova digital e a cooperação entre países é de suma importância para se facilitar a investigação e o combate à cibercriminalidade, já que a prática dos cibercrimes e os efeitos deles decorrentes podem facilmente se alastrar para diversos países.

Nesse sentido, a presente dissertação tem por objetivo tratar do tema da prova digital em Portugal através das normas que regulam essa matéria, bem como apresentar as principais problemáticas de compatibilização e interpretativas delas decorrentes, utilizando-se da doutrina e jurisprudência portuguesas de modo a encontrar a melhor forma de investigação e combate à cibercriminalidade sem prejudicar de forma abusiva os direitos fundamentais[5] das pessoas em prol da busca da verdade e punição dos culpados.

1. Evolução legislativa relativa à criminalidade informática em Portugal: Lei nº 109/91 e Lei nº 109/09

A primeira lei que regulou a matéria de cibercrime em Portugal foi a lei da criminalidade informática, Lei nº 109/91[6], de 17 de agosto que por ter se tornado deficitária, desatualizada, foi expressamente revogada e substituída pela atual lei que regula o tema, a Lei do cibercrime nº 109/2009 de 15 de setembro.

A antiga lei da criminalidade informática tratava apenas do direito substantivo, dos crimes informáticos, sendo as disposições do Código Penal subsidiariamente aplicáveis aos crimes nela previstos, conforme dispunha o artigo 1º, lei 109/91. Já a matéria processual

---

[4] "Salienta-se, efectivamente, que não é hoje possível conseguir a prova (digital) de boa parte dos crimes, informáticos e não só, sem o intercâmbio entre as entre as entidades policiais e judiciárias dos vários países conexionados com a prática desses delitos", MILITÃO, Renato Lopes, "*A propósito da prova...",* p. 262.

[5] "...esta verdadeira revolução tecnológica, ao mesmo tempo que criou facilidades inimagináveis na área da comunicação, potenciou também os riscos de violação da privacidade. Efectivamente, os já mencionados novos meios de comunicação, se permitiriam que esta se realizasse com enorme facilidade, alcançando um variado número de pessoas com uma rapidez estonteante, resultaram também em formas mais susceptíveis de intromissões não desejadas de terceiros.", NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal,* Coimbra Editora, 2011, p. 24.

[6] "Os Estados têm vindo a adoptar medidas visando prevenir e contrariar as práticas ilegais e abusivas nas redes de comunicação. Portugal tem, desde 1991, por impulso da recomendação R (89) 9 do Conselho da Europa, um quadro normativo que visa punir aquilo a que chamou os crimes informáticos: a Lei nº 109/91, de 17 de Agosto. Este diploma, adequado à realidade que se destinava a regular na data em que entrou em vigor, pelo decurso de quase duas décadas, tornou-se deficitário", cfr. exposição de motivos da proposta de Lei nº 289/X/4ª – Lei do Cibercrime, pg. 1. Essa Recomendação nº R (89) 9 de setembro de 1989 continha uma lista mínima e outra facultativa de crimes informáticos, tendo sido na sequência aprovada a Lei nº 109/91 que regulou a criminalidade informática e praticamente copiou os crimes que continham naquela Recomendação, segundo ASCENSÃO, José de Oliveira, "O cibercrime" in: *Direito penal económico e financeiro,* Coimbra Editora, 2012, p. 308.

relativa ao tema era regulada pelo artigo 189º, CPP, que foi estendido[7] com a reforma do CPP em 2007[8] através da Lei nº 48/2007, de 29 de agosto, para abranger a recolha de prova eletrónica, na medida em que o disposto nos artigos 187º, 188º, CPP, relacionados às escutas telefónicas, "é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital e à intercepção das comunicações entre presentes[9]".

Entretanto, ao longo dos anos, a lei 109/91 tornou-se ultrapassada na medida em que foram surgindo novos crimes informáticos[10] que não eram regulados pela lei portuguesa, mas já vinham sendo considerados crimes por legislações europeias e instrumentos internacionais[11]. Do mesmo modo, a lei de 91 não trazia normas processuais[12] específicas no que tange a recolha e conservação de prova digital, sendo utilizado dispositivo do CPP alterado em 2007 para tentar suprir a lacuna existente. Além disso, as normas reguladas no CPP sobre a matéria tornaram-se insuficientes e inadequadas, por se tratar de mera extensão de um regime já existente às telecomunicações. Nesse sentido, concordamos com João Conde Correia que defende que ao "aglutinar diversas realidades, carecidas de graus de

---

[7] "A diversidade de natureza que distancia o telefone do correio electrónico enquanto meio de comunicação é, a nosso ver, impeditivo bastante para concordar com a cláusula de extensão operada no artigo 189º, do CPP", NEVES, Rita Castanheira, *As ingerências nas comunicações*..., p. 172.

[8] "Esta novidade introduzida pela Reforma de 2007 tem sido alvo das mais duras críticas por parte da maioria da doutrina, pois na verdade não faz sentido pensar um regime com base na intercepção de comunicações e depois estender esse mesmo regime a uma situação que já não é comunicação", NEVES, Rita Castanheira, *As ingerências nas comunicações*..., p. 181.
"Na revisão de 2007 do Código de Processo Penal não se encontra sombra de um pensamento abrangente sobre a constelação de problemas suscitados pela prova electrónica ou qualquer sistematização das províncias relativas à intromissão nas telecomunicações e à recolha da prova digital. Grave lacuna num processo de reforma (...)", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", pp. 87-88.

[9] Artigo 189, nº1, CPP.

[10] "É, por exemplo, o caso da produção ou difusão de vírus e outros programas maliciosos, realidades ainda não consagradas na lei nacional... Não obstante, é sobrejamente conhecida a nocividade que resulta da produção e difusão de vírus informáticos pelas redes de comunicações. Essa é a razão pela qual muitas outras legislações optaram pela criminalização desta actividade, na sequência, aliás, da disposição do artigo 6º da Convenção sobre Cibercrime do Conselho da Europa", cfr. Exposição de motivos da proposta de Lei nº 289/X/4ª – Lei do Cibercrime, p. 1.

[11] Exposição de motivos da proposta de Lei nº 289/X/4ª, ..., p. 1.

[12] "Já nos campos das normas de direito processual penal, a desadequação da ordem jurídica nacional às novas realidades a implementar é superior. A recente revisão do Código de Processo Penal optou pela limitação, em abstracto, da possibilidade de realização de intercepções de comunicações telefónicas e electrónicas, não tendo incluído normas especiais para a área da cibercriminalidade. Assim, não está prevista a obtenção de dados de tráfego nem a realização de intercepção de comunicações electrónicas na investigação de crimes não previstos no artigo 187º do Código de Processo Penal", Exposição de motivos da proposta de Lei nº 289/X/4ª, ..., pp. 2-3.

tutela diversos e de distintas exigências práticas, o legislador deu um contributo decisivo para a incerteza e para a insegurança jurídicas e dificultou a tarefa das instâncias formais de controlo[13]".

Assim, conforme dispõe a exposição de motivos da proposta de Lei nº289/X/4ª, lei do cibercrime, importa "superar o actual regime, de modo a fornecer ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual. É o que se pretende fazer por via da lei que agora se propõe[14]".

Assim, é notório que a lei do cibercrime foi inovadora[15], na medida em que além de ter previsto cibercrimes que antes não eram regulados por Portugal, muito embora a maioria deles já tivesse sido regulada na lei 109/91, trouxe conceitos novos como "dados informáticos", "dados de tráfego" e "fornecedor de serviços", bem como normas relativas à cooperação penal internacional que complementam as disposições da Lei 144/99, de 31 de agosto, Lei da Cooperação Judiciária em Matéria Penal. Além disso, trouxe um conjunto de meios de obtenção de provas novos, diferentes, que não existiam até 2009, não estavam previstos na legislação portuguesa, dentre eles a preservação expedita de dados (art. 12º, LCC), a revelação expedita de dados de tráfego (art. 13º, LCC) e a injunção para apresentação ou concessão do acesso a dados (art. 14º, LCC).

Já a pesquisa de dados informáticos[16] (art. 15º, LCC) seria o equivalente às buscas, prevista nos artigos 174º, 251º, CPP; a apreensão de dados informáticos[17] (art. 16º, LCC) corresponderia a apreensão de objetos do art. 178, nºs 1,3, CPP; a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (art. 17º, LCC) equivaleria à apreensão de correspondência prevista nos artigos 179º, 252º, CPP; a intercepção de

---

13 CORREIA, João Conde, "Prova digital: enquadramento legal", in Ebook *Cibercriminalidade e prova digital*, Centro de Estudos Judiciários, julho de 2018, p. 16.

14 Exposição de motivos da proposta de Lei nº 289/X/4ª, ..., p. 3.

15 "Na parte relativa à prova electrónica, a Lei do Cibercrime visou cumprir obrigações do Estado português derivadas da Convenção do Conselho da Europa sobre recolha de prova electrónica suprindo uma lacuna do direito processual geral em termos amplos e abrangentes da generalidade dos crimes", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...," p. 96.

16 "(...) no art. 15º a busca de dados informáticos num sistema informático é apodada de pesquisa, com o que não se altera a sua verdadeira natureza processual de busca.", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 114.

17 "Relativamente à apreensão, apesar de algumas inovações em termos de verbalização das regras (art. 16º), não se alteram os pressupostos funcionais da apreensão em processo penal (cf. art. 178, nº1 e 3, CPP)", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 115.

comunicações (art. 18º, LCC) seria o equivalente ao disposto no regime da intercepção e gravação de conversações ou comunicações telefónicas[18] constante dos artigos 187º a 190º, CPP e as acções encobertas[19] (art. 19º, LCC) vieram alargar o âmbito de admissibilidade das mesmas já previstas na Lei 101/2001, art. 2º. É importante destacar que os artigos 18º e 19º, LCC, por preverem os meios de obtenção de prova mais intrusivos possuem uma aplicação mais reduzida comparada aos outros[20]. Assim, muito embora algumas figuras processuais da lei do cibercrime já existissem por estarem previstas no CPP, foram adaptadas aos crimes informáticos, ao ambiente digital[21].

Nesse sentido, percebe-se que quando a lei do cibercrime entrou em vigor houve uma dificuldade em saber qual diploma seria aplicado à recolha de prova electónica, o artigo 189º, nº1, CPP ou as disposições processuais previstas na nova lei 109/2009 e reguladas do artigo 11º ao artigo 19º. Entretanto, essa questão controversa já foi pacificada e será tratada mais afundo na sequência da dissertação.

Conforme dispõe artigo 1º, Lei 109/09, ela "estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa".

---

[18] "Do mesmo modo, foi adaptado para este diploma o regime de intercepção de comunicações, previsto no Código de Processo Penal para as comunicações telefónicas", Exposição de motivos da proposta de Lei nº 289/X/4ª, ..., p. 5.

[19] "Uma originalidade nacional que não decorreu de qualquer previsão da Convenção do Conselho da Europa, nem da Decisão-Quadro, e que se apresenta dividida em duas normas autónomas (...), MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 126.

[20] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018, p. 18.

[21] "Na verdade, a essência destas medidas processuais coincide, no ambiente do ciberespaço, com as clássicas formas de busca e apreensão, do processo penal. Porém, a forma como a busca e a apreensão estão descritas no Código de Processo Penal exigiam alguma adequação a estas novas realidades", Exposição de motivos da proposta de Lei nº289/X/4ª, ..., p. 5.

1.1. Convenção sobre o Cibercrime do Conselho da Europa de 2001

Em Budapeste, no dia 23 de novembro de 2001, Portugal assinou a Convenção sobre o Cibercrime do Conselho da Europa[22] que foi aprovada, e veio a ratificá-la posteriormente, com reservas (no que tange a matéria de extradição), apenas no dia 15 de setembro de 2009, através da Resolução da Assembleia da República nº 88/2009 e do Decreto do Presidente da República nº91/2009[23]. Essa Convenção, segundo a exposição de motivos da proposta de lei nº289/X/4ª, lei do cibercrime, "é o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço. Tem vocação universal e pretende-se que venha a ser aceite pela generalidade dos países do Mundo. Pretende harmonizar as várias legislações sobre a matéria, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal. Incide sobre direito penal material (...) mas inclui também medidas processuais e de cooperação judiciária internacional[24]".

Dessa forma, a lei 109/91, encontrava-se deficitária e precisava ser modificada para se adequar à nova realidade e às exigências internacionais. Nesse sentido, a lei 109/09, lei do cibercrime que revogou expressamente a anterior, foi adaptada à Convenção sobre Cibercrime do Conselho da Europa, o que está expressamente disposto no artigo 1º, lei 109/09, prevendo normas de direito substantivo, processuais e de cooperação penal internacional relativas ao cibercrime.

Segundo o preâmbulo[25] da Convenção sobre o Cibercrime do Conselho da Europa, além de haver uma preocupação com a harmonização das legislações nacionais referentes ao cibercrime de modo que possa haver uma cooperação internacional com recolha electrónica de prova que facilite e torne mais eficaz a investigação e o combate à criminalidade digital, a Convenção preocupou-se também com "a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano, tal como garantidos pela Convenção para a Protecção dos

---

[22] "A Convenção foi promovida pelo Conselho da Europa e não diretamente pela Comunidade Europeia – decerto porque ao tempo se negava a competência da Comunidade em matéria penal", ASCENSÃO, José de Oliveira, "O cibercrime...", p. 310.

[23] Informação disponível em http://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0 <acedido a 9-03-19>

[24] Exposição de motivos da proposta de Lei nº289/X/4ª, ..., p. 2.

[25] Cfr. Relatório explicativo da Convenção do Cibercrime, STE nº 185.

Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, pelo Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como por outros tratados internacionais aplicáveis em matérias de direitos do Homem (...) e, ainda, o direito ao respeito pela vida privada. Tendo igualmente presente o direito à protecção de dados pessoais, tal como é conferido, por exemplo, pela Convenção do Conselho da Europa de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal[26]", o que foi reiterado no artigo 15, nº1 da referida Convenção.

Nesse sentido, a Convenção previu definições, normas de direito penal material, ou seja, crimes informáticos, bem como formas de responsabilidade e sanções, além de normas de direito processual penal, de competência e de cooperação internacional que deveriam ser adotadas pela legislação interna de cada um dos Estados-Membros como forma de se alcançar os objetivos da referida Convenção: a harmonização das leis relativas ao cibercrime de modo que se facilite a sua investigação, punição e combate.

1.2. Decisão-Quadro nº 2005/222/JAI e Directiva 2013/40/EU

A Decisão-Quadro nº2005/222/JAI do Conselho da União Europeia de 24 de fevereiro de 2005 relativa a ataques contra os sistemas de informação que foi transposta para a lei do cibercrime portuguesa, veio a ser substituída pela Directiva 2013/40/EU do Parlamento Europeu.

O objetivo da referida decisão-quadro, segundo o considerando (1) é "reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação[27]".

Assim, de forma semelhante à Convenção sobre o Cibercrime do Conselho da Europa

[26] *Idem*

[27] "Há provas de ataques contra os sistemas de informação, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação que constituem a infra-estrutura vital dos Estados-Membros. Esta ameaça poderá comprometer a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia", cfr. dispõe Considerando (2) da Decisão-Quadro nº2005/222/JAI.

de 2001, a decisão-quadro de 2005 também tem por escopo harmonizar[28], aproximar as legislações nacionais penais de modo que se possa facilitar a cooperação internacional de combate aos ataques contra os sistemas de informação, praticados principalmente através do terrorismo e da criminalidade organizada. Reiterando esse posicionamento, o considerando (3) da referida decisão-quadro dispõe que "uma resposta eficaz a essas ameaças pressupõe uma abordagem global em matéria de segurança das redes e da informação (...)".

Nesse sentido, a decisão-quadro traz definições, prevê crimes e sanções relacionados aos ataques contra os sistemas de informação que devem ser seguidos por todos os Estados-Membros signatários em suas respetivas legislações penais de modo que se possa dar efetividade à cooperação judiciária e policial no combate ao terrorismo e à criminalidade organizada.

A Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013 que também é relativa a ataques contra os sistemas da informação, conforme disposto em seu considerando (34) "(..) visa alterar e alargar o âmbito das disposições da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação. Dado que as alterações a introduzir são numerosas e substanciais, a Decisão-Quadro 2005/222/JAI deverá, por uma questão de clareza, ser integralmente substituída no que se refere aos Estados-Membros que participam na adoção da presente diretiva".

Reiterando essa questão, o artigo 15º da referida Diretiva dispões que "a Decisão-Quadro 2005/222/JAI é substituída, no que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, sem prejuízo das obrigações dos Estados-Membros quanto ao prazo de transposição daquela decisão-quadro para o direito nacional. No que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, as remissões para a Decisão-Quadro 2005/222/JAI devem entender-se como sendo feitas para a presente diretiva."

Nesse sentido, muito embora a decisão-quadro tenha sido substituída pela diretiva

[28] "As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio", segundo considerando (5) da Decisão-Quadro 2005/222/JAI.

devido a alterações numerosas e substanciais, percebe-se que o objetivo principal continua a ser o mesmo, qual seja, "aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes (...)", conforme considerando (1) da Diretiva 2013/40/UE e artigo 1º da mesma.

É importante salientar que a lei 109/2009 transpôs a decisão-quadro 2005/222/JAI de 2005 para a ordem jurídica interna e ainda não sofreu alterações, ou seja, a lei do cibercrime ainda não foi adaptada à Diretiva 2013/40/UE de 2013 que acabou por substituir a referida decisão-quadro. No entanto, percebe-se que não é necessário que modificações sejam feitas já que a lei do cibercrime foi além das disposições da referida decisão-quadro, regulando tudo que se encontra na nova Diretiva 2013/40/UE. Assim, estamos de acordo com Armando Dias Ramos que dispõe que "no domínio das infrações penais a Diretiva ora aprovada acaba por não ser inovadora, pelo menos face à nossa atual legislação[29]".

1.3. Lei nº32/2008

Outra lei importante no âmbito da criminalidade informática em Portugal é a Lei nº32/2008 que segundo artigo 1º "regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Diretiva nº 2006/24/CE[30] do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (...)".

É importante também salientar que o artigo 1º, nº2 da referida lei nº 32/2008 dispõe que "a conservação de dados que revelem o conteúdo das comunicações é proibida, sem

---

[29] RAMOS, Armando Dias, *A novíssima Diretiva relativa ao Cibercrime,* 2013, disponível em https://www.academia.edu/8696174/A_Nov%C3%ADssima_Diretiva_sobre_o_Cibercrime > acedido a 25-04-19.

[30] Para maiores informações, consultar RAMALHO, David/COIMBRA, José, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *O Direito*, 147, 2015, pp. 1006-1007.

prejuízo do disposto na Lei nº 41/2004, de 18 de agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações".

Nesse sentido, percebe-se que apesar de haver uma preocupação com a conservação e transmissão de dados de tráfego e de localização de modo que se facilite a investigação e a punição relativas à cibercriminalidade, essa conservação e transmissão não podem dizer respeito ao conteúdo das comunicações, nem podem ser feitas em qualquer situação e por períodos indeterminados, deve-se observar as categorias[31] de dados a conservar, bem como obedecer a certas condições[32] e períodos de conservação[33], como forma de proteger os direitos fundamentais das pessoas, como os dados pessoais e a privacidade, regulados pela Lei nº41/2004 no que se refere às telecomunicações.

A própria Convenção sobre o cibercrime que serviu de base para as legislações de vários países no que tange a essa matéria, em seu preâmbulo e artigo 15º destacam a importância da proteção adequada dos direitos do homem e de suas liberdades fundamentais, como a vida privada e dados pessoais, sendo necessário "garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano[34]".

No mesmo sentido, a Diretiva 2013/40/UE que substituiu a decisão-quadro 2005/222/JAI nos seus considerandos (29) e (30) demonstra preocupação com o respeito aos direitos humanos e as liberdades fundamentais das pessoas, como a proteção dos dados pessoais (consagrados pelo artigo 16º, nº1, TFUE e artigo 8º da Carta dos Direitos Fundamentais da União), o respeito da vida privada, a liberdade de expressão e de informação, presunção de inocência, direitos de defesa, dentre outros. Da mesma forma, encontra-se na lei 109/2009 o artigo 30º que regula a proteção de dados pessoais de acordo com o disposto na Lei nº 67/98.

Assim, muito embora a conservação e transmissão de certos dados sejam essenciais à investigação e ao combate do cibercrime, há certos limites que devem ser respeitados como forma de salvaguarda dos direitos fundamentais das pessoas, devendo ser feita uma

---

[31] Artigo 4º, Lei 32/2008.

[32] Artigo 9, nº1, Lei 32/2008.

[33] Cfr. considerando (6), Diretiva 2006/24/CE do Parlamento Europeu e do Conselho de 15-03-06. Artigo 6º, Lei 32/2008 dispõe que "as entidades referidas no nº1 do artigo 4º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação".

[34] Relatório explicativo da Convenção do Cibercrime, STE nº 185.

ponderação entre a aplicação da lei e a proteção dos direitos fundamentais através do princípio da proporcionalidade.

No que diz respeito a Diretiva 2006/24/CE relativa à conservação de dados que foi transposta pela lei 32/2008, o TJUE a declarou inválida em 2014[35] pelo facto dele considerar que "ao impor a conservação desses dados e ao permitir o acesso às autoridades nacionais competentes, a diretiva imiscui-se de forma especialmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais. Além disso, o facto de a conservação e posterior utilização dos dados serem efetuadas sem que o assinante ou o utilizador inscrito seja informado é suscetível de gerar nas pessoas em causa a sensação de que a sua vida privada é objeto de vigilância constante[36]".

O TJUE vem então a elencar uma série de razões pelas quais considera a diretiva inválida, dentre elas o facto da diretiva "abranger de forma generalizada todos os indivíduos, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada uma diferenciação, limitação ou exceção em função do objetivo da luta contra os crimes graves (...) Por outro lado, o Tribunal de Justiça constata que a diretiva não prevê garantias suficientes que permitam assegurar uma proteção eficaz dos dados contra os riscos de abusos bem como contra qualquer acesso e qualquer utilização ilícitos dos dados (...)[37]".

Desse modo, percebe-se que o TJUE "reconhece que as medidas previstas na Diretiva (...) são legítimas e adequadas ao fim visado. Mas, quanto a necessidade de tais medidas, conclui pela violação do princípio da proporcionalidade nessa vertente[38]". Assim, considerou que a diretiva não respeitou a proteção dos direitos fundamentais das pessoas garantidos pela Carta de Direitos Fundamentais da União Europeia[39], restringindo-os (vida privada e proteção de dados pessoais) no que se refere a conservação de dados, sendo, por isso, invasiva e declarada inválida, cuja produção de efeitos é retroativa, a partir da data de entrada em vigor da diretiva. Segundo David Ramalho, "a decisão do TJ marca, assim, o início de uma nova

---

[35] Ac. TJUE no caso *Digital Rights Ireland* – Processo nº C-293/12 e C-594/12.

[36] Cfr. Comunicado de Imprensa nº 54/14 do TJUE, disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054pt.pdf <acedido a 12-03-19>

[37] Cfr. Comunicado de Imprensa nº 54/14 do TJUE, ..., <acedido a 12-09-19>

[38] CALVÃO, Clara Guerra e Filipa; *Fórum de Proteção de Dados, Em foco o novo quadro legal europeu, Anotação*, Comissão Nacional de Proteção de Dados, nº1 de julho, 2015, p. 80.

[39] "A declaração de invalidade tem por fundamento a violação do princípio da proporcionalidade na restrição que a Diretiva opera dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia (UE)", CALVÃO, Clara Guerra e Filipa; *Fórum de Proteção de Dados*..., p. 79.

fase no Direito da União Europeia em matéria de proteção de dados e, no que aqui releva, de conservação de dados de tráfego, assim restaurando a primazia do polo referente ao direito à reserva da intimidade da vida privada e à proteção dos dados pessoais, em detrimento do polo focado na segurança[40]".

No âmbito do direito interno português o problema que surge com a declaração de invalidade da referida diretiva é saber se a lei 32/2008 que a transpôs deve continuar em vigor ou não. Há duas interpretações[41], uma que diz que a declaração de invalidade não tem força obrigatória geral, valeria apenas perante os Estados (Irlanda e Áustria)[42] que colocaram as questões prejudiciais (eficácia *inter partes*) e pretendiam anular a disposição nacional que transpôs a diretiva para seu direito interno. Já a outra defende que a declaração de invalidade teria força obrigatória geral, valeria para todos os Estados (eficácia *erga omnes*).

Porém, o TJUE em nota esclarece que os próprios Estados membros devem regular as questões em causa ao dispor que "o Tribunal de Justiça não resolve o litigio nacional. Cabe ao órgão jurisdicional nacional decidir o processo em conformidade com a decisão do Tribunal de Justiça[43]". Nesse sentido, a lei 32/2008 portuguesa que é mais protetora[44] que a diretiva ainda continua em vigor, não foi alterada[45], apesar da diretiva ter sido considerada inválida[46]. Um exemplo prático em Portugal que comprova essa questão foi a decisão do TC no Acórdão nº 420/2017 de 13 de julho[47].

---

[40] RAMALHO, David/COIMBRA, José, "A declaração de invalidade da Diretiva 2006/24/CE...", p. 1008.

[41] Para maiores esclarecimentos, RAMALHO, David/COIMBRA, José, "A declaração de invalidade da Diretiva 2006/24/CE...", pp. 1018-1024.

[42] Cfr. Comunicado de Imprensa nº 54/14 do TJUE... <acedido a 12-03-19>

[43] Cfr. Comunicado de Imprensa nº 54/14 do TJUE, ... <acedido a 12-03-19>

[44] "Começa-se por notar que a Lei nº 32/2008, ao contrário da Diretiva, especifica os crimes cuja prevenção, deteção e repressão justifica a imposição deste tratamento de dados pessoais (...), e sujeita ainda a controlo judicial prévio o acesso aos dados pelas autoridades competentes (...). Todavia, outros aspetos de regime sobre os quais incide o juízo de invalidade do Tribunal encontram-se previstos também na Lei nacional". CALVÃO, Clara Guerra e Filipa; *Fórum de Proteção de Dados...* p. 80.

[45] "Portugal é um dos 16 Estados-Membros nos quais se tem entendido que a decisão de 8 de Abril de 2014 não interferiu no quadro legal vigente. Com efeito, desde logo no campo legislativo, não foi sentida necessidade de introdução de qualquer alteração normativa – não foi mesmo apresentada, até a data, nenhuma iniciativa legislativa a este propósito", *Nota Prática nº 7/2015*, Gabinete do Cibercrime.

[46] "A declaração de invalidade da Diretiva não implica diretamente a invalidade da lei nacional que a transponha, mas é imperativo avaliar a conformidade desta com o Direito da União Europeia, em especial a Carta dos Direitos Fundamentais da UE", CALVÃO, Clara Guerra e Filipa; *Fórum de Proteção de Dados...*, p. 79.

[47] "Os questionamentos que antecederam a entrada em vigor da Diretiva 2006/24/CE, mantiveram-se ou intensificaram-se para além desta data, tendo designadamente originado decisões em matéria de constitucionalidade por parte dos tribunais de alguns Estados-Membros", Ac. TC nº 420/2017, ponto 12.

1.3.1. Acórdão do Tribunal Constitucional nº 420/2017, de 13 de julho

Foi através do ac. do TC nº 420/2017 que o Estado português discutiu a constitucionalidade do artigo 6º da lei 32/2008 tendo como base comparativa os argumentos apresentados pelo TJUE no acórdão[48] em que declarou a invalidade da Diretiva nº 2006/24/CE que foi transposta para o direito interno através da referida lei portuguesa.

No caso decidido pelo TC, em questão estava um indivíduo suspeito da prática do crime de pornografia de menores. Nesse sentido, o MP veio requerer ao juiz da instrução com fundamento no artigo 9º, nºs 1, 2, conjugado com o artigo 2º, nº1, g, que define crime grave, ambos da lei 32/2008, autorização para a transmissão de dados referentes ao endereço IP do utilizador de modo que ele pudesse ser identificado com base no artigo 4º, nº1, a e nº 2, b, iii, lei 32/2008.

Este pedido foi indeferido pela 1ª Secção de Instrução Criminal da Instância Central da Comarca de Lisboa pelo facto do artigo 6º, lei 32/2008 (faz referência ao artigo 4º) ter sido considerado inconstitucional por contrariar os artigos 18º, nº2, 32º, nº8 e 34º, nº4, CRP que protegem os direitos fundamentais das pessoas dentre eles reserva da intimidade da vida privada, inviolabilidade do domicílio e sigilo da correspondência e das telecomunicações, que só podem ser restringidos para salvaguardar outros direitos constitucionalmente protegidos, com base no princípio da proporcionalidade, mais especificamente a necessidade, conforme artigo 18º, nº2, CRP.

MP então recorre dessa decisão ao TC, que decide que o artigo 6º, lei 32/2008 não é inconstitucional[49] pelo facto do artigo 34º, nº4, CRP proteger o sigilo das telecomunicações no que tange ao conteúdo das comunicações e aos dados de tráfego, mas não engloba os dados de base, o que foi solicitado pelo MP (endereço de protocolo IP do utilizador para que este pudesse ser identificado).

---

48 Ac. TJUE no caso *Digital Rights Ireland* – Processo nº C-293/12 e C-594/12.

49 "Assim, decorre da jurisprudência do Tribunal Constitucional sobre esta matéria que a proteção conferida pelo nº4, art. 34, CRP não abrange os dados de base, como os abrangidos pela norma do presente processo. De facto, os dados relativos à mera identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP não estão abrangidos pelo âmbito de proteção do sigilo das comunicações consagrado naquele preceito constitucional pois não pressupõe um ato de comunicação específico. Não se acompanha, portanto, o juízo do tribunal a quo, quanto à violação do nº4 do art. 34, CRP", cfr. dispõe Ac. TC nº 420/2017, Processo nº 917/16, ponto 12.

No entanto, ressalva que os dados de base são protegidos pelo artigo 26º, CRP[50], que trata dos direitos pessoais, dentre eles a reserva da intimidade da vida privada. Quanto a este aspeto entende o TC que esse direito pessoal em questão também não foi restringido pelo artigo 6º, lei 32/2008 por não ter violado o artigo 18º, nº2, CRP, com base no princípio da proporcionalidade[51], ou seja, a medida restritiva em causa (conservação e transmissão do endereço IP, dado de base) não é desproporcional à restrição da proteção da vida privada[52], por ser uma medida adequada, necessária e justa ao fim pretendido: investigação e punição do responsável pelo crime grave de pornografia de menores.

Nesse sentido, é importante salientar a classificação[53] feita pelo TC entre dados de base, de tráfego e de conteúdo: os dados de base são os "relativos à conexão à rede", os dados de tráfego estão definidos no artigo 2º, nº1, d, Lei 41/2004, definição esta que foi modificada pela lei 109/09, artigo 2º, als. b, c, e são considerados pelo TC como "os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização da rede, data e hora, frequência)" e os dados de conteúdo são os "relativos ao conteúdo da comunicação ou da mensagem".

Acrescenta ainda o TC que "os elementos inerentes à comunicação podem, por outro lado, estruturar-se numa composição sequencial em quatro tempos: a fase prévia à comunicação, o estabelecimento da comunicação, a fase da comunicação propriamente dita e a fase posterior à comunicação. No primeiro tempo relevam essencialmente os dados de base, enquanto que nos restantes importa essencialmente a consideração dos dados de tráfego e de conteúdo"[54].

Dessa forma, como o MP solicitou autorização para obter a transmissão de dados de base conservados pelos fornecedores de serviços de comunicações eletrónicas e não de tráfego ou de conteúdo, não há que se falar que o artigo 6º da lei 32/2008 é inconstitucional

---

[50] Ac. TC nº 420/2017, ponto 13.

[51] "O princípio da proporcionalidade ocupa lugar central na avaliação dos requisitos materiais exigidos nas restrições de direitos fundamentais (...). Importa, pois, começar por identificar o interesse público prosseguido pela norma sindicada. No presente caso, o interesse público é a 'investigação, deteção e repressão de crimes graves por parte das autoridades competentes', tal como previsto no artigo 1º, nº1 da Lei 32/2008 (...). A salvaguarda da legalidade democrática e a ação penal, nomeadamente contra os crimes referidos, constituem interesses públicos com proteção constitucional.", cfr. Ac. TC nº 420/2007, ponto 13.

[52] Ac. TC nº 420/2017, ponto 14.

[53] Classificação tripartida do TC no Ac. nº 420/2017, ponto 5 com base no acórdão nº403/2015, ponto 9.

[54] Ac. TC nº 420/2017, ponto 5.

por violação do artigo 32º, nº4, CRP.

No mesmo sentido, o TC indica que a Lei nº 32/2008 também não é inconstitucional por ter previsto diversas normas que não foram reguladas pela diretiva, indo para além desta, já que "estipulou regras de acesso aos dados, sujeitando-o a critérios de necessidade, adequação e proporcionalidade, a verificar inclusivamente no que respeita à definição das categorias de dados (nº 1 e 4 do artigo 9º) e limitando-o a um catálogo restrito de titulares dos dados (nº3 do artigo 9º); definiu o conceito de crimes graves (alínea g do nº1 do artigo 2º); impôs a precedência de mandado judicial no acesso aos dados, mediante requerimento do MP ou da autoridade de polícia criminal competente (nº2, artigo 9º); estabeleceu particulares deveres de proteção e segurança dos dados, tendo, inclusivamente, criado uma aplicação informática denominada 'sistema de acesso ou pedido de dados às operadoras de comunicações' (SAPDOC), (...), nº3 do artigo 7º da Lei nº 32/2008 e Portaria nº 469/2009 e sujeitou expressamente a decisão judicial de transmitir os dados ao dever de respeitar o segredo profissional nos termos legalmente previstos, apesar de não evitar a sua conservação (nº4 do artigo 9º)[55]". A Lei nº 32/2008 também previu no seu artigo 7º, nº1, al. e) que os dados no final do período de conservação devem ser destruídos, o que contribui para justificar a decisão do TC de que o artigo 6º da mesma lei não é considerado inconstitucional.

2. Prova Digital[56] X Proteção de Direitos Fundamentais

Conforme já explicitado, devido a necessidade de regular crimes informáticos novos, bem como disposições processuais específicas e de cooperação internacional relativos a essa matéria, a lei 109/2009, atual lei do cibercrime, surgiu e revogou a antiga, lei 109/91, substituindo-a.

Essa lei do cibercrime, no que se refere ao tema da recolha e conservação de prova digital, foi inovadora na medida em que trouxe meios de obtenção de provas[57] que até sua

---

[55] Ac. TC nº 420/2017, ponto 11.

[56] "De entre as classificações feitas pelo legislador, poderemos incluir a prova digital como prova pericial, por a mesma exigir especiais conhecimentos técnicos para a sua perceção ou apreciação dos factos. Poderá também classificar-se a prova digital como prova documental, sempre que a mesma possa ser corporizada em escrito ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico", RAMOS, Armando Dias, *A prova digital em processo penal: o correio eletrónico,* Chiado editora, 2014, p. 86.

[57] Sobre a distinção entre meios de obtenção da prova e meios de prova consultar ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2ª edição, 2019, pp. 114-133.

entrada em vigor não existiam, como os tratados nos artigos 12º, 13º e 14º, LCC. Também regulou figuras processuais que já estavam previstas na legislação portuguesa, mas foram adaptadas aos crimes informáticos, ao ambiente digital, encontradas do artigo 15º ao 19º, LCC.

Segundo Benjamim Silva Rodrigues a "prova electrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada em repositório electrónico-digitais de armazenamento ou transmitida em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital[58]".

Nesse sentido, percebe-se que o tema prova digital é de suma importância no que tange a investigação e responsabilização dos criminosos, e que os avanços tecnológicos permitiram o surgimento de novos meios de produção de prova que até então eram impensáveis, como registo de imagens, filmagens, escutas, gravações, análise genética, dentre outros[59]. Em contrapartida, conclui Renato Lopes Militão que "se está perante uma prova fragmentária[60], dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invisível e espacialmente dispersa. Sendo, por isso, extremamente difícil, complexo, e, até, aleatório detectar, preservar, apreender, analisar, tratar, garantir a fiabilidade, assegurar a compreensibilidade a apresentar em julgamento as provas digitais[61]", o que dificulta as investigações[62] e o combate à cibercriminalidade, sendo necessário normas que regulem eficazmente[63] e de forma autónoma a recolha de prova digital, tal como o fez a lei 109/2009, mas deveria ter feito o CPP[64].

---

[58] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital e da criminalidade informático-digital"; *Da prova penal*, Tomo IV, 2011, p. 39.

[59] MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 85.

[60] Para maiores esclarecimentos acerca dessas características da prova eletrónico-digital consultar RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", pp. 41-44.

[61] MILITÃO, Renato Lopes, "*A propósito da prova digital*...", p. 261.

[62] "(...) cerca de 20% dos inquéritos em investigação ou investigados nesta área (da criminalidade informática) são concluídos com proposta de arquivamento por inexistência de elementos que permitam prosseguir a investigação (...)", MILITÃO, Renato Lopes, "*A propósito da prova digital*...", p. 261.

[63] MILITÃO, Renato Lopes, "*A propósito da prova digital*...", p. 263.

[64] "(...) as normas referentes à obtenção da prova digital devem ser delineadas à luz e no quadro do regime geral de obtenção da prova. Sem prejuízo, como já dissemos, de algumas adaptações, face a certas particularidades daquele tipo específico de prova. Por isso, do nosso ponto de vista, aquelas normas devem integrar-se no CPP. Só deste modo se conseguirá alcançar a sua necessária harmonização com o regime geral de obtenção das provas. Para além das demais vantagens decorrentes da codificação, (...)", MILITÃO, Renato Lopes, "*A propósito da prova digital*...", p. 266.

Ainda, segundo Paulo Dá Mesquita, "no plano processual penal o desenvolvimento tecnológico implicou duas linhas problemáticas novas em relação a velhos modelos probatórios: a intromissão em comunicações que de outra forma não seriam conhecidas e a fixação do acontecimento em que os dispositivos tecnológicos registam os dados para o futuro[65]". Já conforme Costa Andrade, seriam "métodos ocultos de investigação (...), métodos intrusivos que não têm de ser ocultados ao visado, pelo menos na fase de execução da recolha da prova em suporte electrónico[66]".

Nesse mesmo sentido, concordamos com Militão ao verificar que "a Lei nº 109/2009, com vista à obtenção de prova digital, consagrou múltiplos e extensíssimos meios processuais, deveres para terceiros e mecanismos de cooperação internacional profundamente agressivos, intrusivos, desleais e perigosos[67]". No entanto, é importante salientar que a lei do cibercrime previu as buscas tradicionais no art. 15º, mas não as buscas online, por não admiti-las, já que, conforme Rita Neves[68], seria um método oculto de investigação, segundo o qual os dados informáticos do computador do visado seriam recolhidos ocultamente, sem que ele tivesse conhecimento, a não ser que houvesse um dever de notificação *a posteriori*.

Assim, muito embora a lei do cibercrime tenha sido inovadora e de suma importância no combate à cibercriminalidade, ao mesmo tempo trata-se de uma lei perigosa que pode vir a ferir direitos, garantias e liberdades. Dessa forma, a utilização dos meios de prova nela previstos, não pode ser indiscriminada, o que afetaria os direitos fundamentais das pessoas[69], como a vida privada e dados pessoais, que são constitucionalmente protegidos em diversos artigos como 18º, nº2[70]; 26º; 32º, nºs 2, 8; 34º, nº4, CRP, dentre outros. Nesse sentido dispõe

---

65 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 84.

66 ANDRADE, Manuel da Costa, in "Prolegómenos sobre prova electrónica...", p. 85.

67 MILITÃO, Renato Lopes, "*A propósito da prova digital*...", p. 274.

68 NEVES, Rita Castanheira, *As ingerências nas comunicações*..., pp. 198, 284, 351.

69 "(...) a concretização de tais medidas ofende, acrescida e gravemente, múltiplos direitos, liberdades e garantias, não só dos agentes dos crimes mas também, pelo menos em boa parte dos casos, de suspeitos inocentes ou terceiros acidentais (...). Por outro lado, frequentemente, a prova digital tem que ser obtida em sistemas informáticos de terceiros, máxime das operadoras de comunicação. O que igualmente ofende direitos destas. Para além de degradar obrigações contratuais e legais das mesmas, designadamente o dever de sigilo, o qual, em regra, protege relevantíssimos valores sociais e subjectivos", MILITÃO, Renato Lopes, "*A propósito da prova digital*...", pp. 267-268.

70 "Além de precisarem de autorização constitucional, as restrições de direitos fundamentais carecem também de justificação, não podendo legitimar-se senão pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos e não podendo ultrapassar a medida necessária para o efeito (art. 18º, nº2) (...). A regra de solução do conflito é a da máxima observância dos direitos fundamentais envolvidos e da sua

acertadamente Militão que "assiste-se, na verdade, a uma progressiva degradação das garantias processuais do suspeito e do arguido. De facto, a diminuição das garantias processuais é um dos aspectos que mais rapidamente se manifestam enquanto características do Estado punitivo. Efectivamente, sobreposto o valor segurança ao bem liberdade, os direitos fundamentais tendem a constituir um obstáculo numa luta eficaz do Estado contra a criminalidade. Assim, o processo penal neoliberal é cada vez mais secretista, imediatista, intrusivo e desleal[71]". Acrescenta ainda Militão que "em virtude das referidas acções de investigação criminal, informação de múltipla natureza chega ao conhecimento de um número elevado de pessoas indeterminadas. Ora, esta situação gera enormes riscos de a informação vir a ser utilizada fora dos procedimentos respectivos, para finalidades alheias a estes[72]".

Assim, como forma de se evitar intromissões descabidas, segundo Paulo Dá Mesquita, exige-se "uma reconstrução conceptual complexa, com um enquadramento teórico que se adapte à rotura epistemológica introduzida pelas novas tecnologias no processamento, captação e memória nas comunicações[73]". Caso contrário, podem surgir problemas como o que já foi analisado no ac. TC nº 420/2017, segundo o qual foi discutida a constitucionalidade do artigo 6º, lei 32/2008 que seria um meio de prova que teria violado direitos fundamentais das pessoas (comprovou-se que não).

Entende João Correia que os direitos fundamentais devem ser protegidos, mas não podem ser absolutos[74], já que "a máxima protecção dos direitos fundamentais colocaria barreiras intransponíveis a descoberta da verdade e, em consequência, à realização da justiça e a busca da verdade a todo custo eliminaria os mais elementares direitos, conduzindo a uma mistificação da justiça. Este conflito revela-se, em toda a sua amplitude, de forma exponencial, no domínio dos meios de prova e de obtenção da prova. Com efeito, o interesse

---

mínima restrição compatível com a salvaguarda adequada do outro direito fundamental ou outro interesse constitucional em causa", MILITÃO, Renato Lopes, "*A propósito da prova digital...*", p. 270.

71 MILITÃO, Renato Lopes, "*A propósito da prova digital...*", p. 255.

72 MILITÃO, Renato Lopes, "*A propósito da prova digital...*", p. 268.

73 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", pp. 84-85.

74 "Efectivamente, os direitos fundamentais não são absolutos, podendo ser restringidos nos casos expressamente previstos na Constituição (art. 18º, nº2, 1ª parte). Esta autorização expressa legitima a actividade restritiva do legislador ordinário e dá segurança jurídica aos cidadãos, na medida em que apenas nesses casos poderá haver compressão dos direitos fundamentais", CORREIA, João, "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32, nº8, 2ª parte da CRP?)", *Revista do MP*, nº 79, 1999, p. 59.

punitivo do Estado e a plêiade de métodos (...) podem afrontar, de forma grave e irreversível, os direitos fundamentais inerentes a um ser livre e digno[75]". Nesse sentido, segundo artigo 32º, nº8, CRP são nulas todas as provas obtidas mediante abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações, e não podem ser utilizadas, sendo consideradas provas proibidas[76], conforme art. 126º, nº3, CPP.

Assim, enquanto não surgem alterações legislativas de melhorias na matéria, devem ser respeitadas as regras, os critérios e as condições existentes nas leis que regulam e permitem a recolha e a conservação de prova digital. Da mesma forma, concordamos com Figueiredo Dias[77], segundo o qual o juiz ao avaliar em um caso concreto se uma prova é válida ou não, deve aplicar o princípio da proporcionalidade[78] ou proibição do excesso[79] (na sua vertente necessidade), consagrado no artigo 18º, nº2, CRP[80], como forma de ponderação[81] das valorações conflituantes, de controlo da necessidade ou não de haver intromissões na vida privada das pessoas em prol da produção de uma dada prova para a descoberta da verdade e realização da justiça. Assim, evita-se a violação abusiva dos seus direitos fundamentais como a reserva da intimidade e da vida privada[82], inviolabilidade e sigilo das

---

75 CORREIA, João, "Qual o significado de abusiva intromissão...", p. 46.

76 Para maiores esclarecimentos, DIAS, Jorge de Figueiredo, "Revistação de algumas ideias- mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)", *Revista de Legislação e de Jurisprudência*, 146 (2016), pp. 3-16.

77 DIAS, Jorge de Figueiredo, "Revistação de algumas ideias...", pp. 9-10.

78 CANOTILHO, J.J Gomes; MOREIRA, Vital, *Constituição da República Portuguesa anotada*, Vol. I, Coimbra Editora, 1ª edição brasileira, 4ª edição portuguesa revista, 2007, pp. 392-393.

79 "Nesse quadro, sem prejuízo da inconstitucionalidade material de múltiplas normas daqueles diplomas, exige-se uma redobrada ponderação dos valores em jogo em sede de interpretação e aplicação de todos os seus dispositivos por parte das autoridades competentes, as quais deverão aplicar efectivamente o princípio da proibição do excesso. Para além de se exigir igualmente particular cautela por parte do julgador na apreciação das provas digitais, máxime as indiciárias, dada a fragilidade desta prova", MILITÃO, Renato Lopes, "*A propósito da prova digital...*", p. 281.

80 "A intervenção restritiva do legislador ordinário terá que constar de lei ou decreto-lei autorizado, com caráter geral e abstracto e não retroactivo (...). Tem, ainda, que ser adequada, ou seja, apropriada aos fins que se propõe atingir, necessária, na medida em que só é admissível quando for impossível utilizar outro meio menos oneroso, e proporcional em relação aos resultados obtidos. É o chamado princípio da proibição do excesso (art. 18, nº2, CRP)", CORREIA, João, "Qual o significado de abusiva intromissão...", p. 59.

81 Em sentido contrário e em posição minoritária, ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 2013, p. 201.

82 "Assim, pode-se dizer que a vida privada compreende aqueles factos, atitudes ou opiniões individuais e particulares, que não tenham qualquer relação com a vida pública e que possam, em determinado momento histórico, ser razoavelmente considerados confidenciais, por forma a impedir ou restringir a sua divulgação", CORREIA, João, "Qual o significado de abusiva intromissão...", p. 49.

comunicações[83], a proibição de autoincriminação, dentre outros.

Superada essa dificuldade, é notório que com o surgimento de uma lei nova (lei 109/2009) que regula matérias novas, a mesma fica suscetível a ocorrência de incompatibilizações[84] com normas já existentes, como aconteceu entre a lei do cibercrime, o CPP e a lei 32/2008, o que será analisado a seguir e está em conformidade com João Correia que dispõe que "o legislador nacional continua a manter em vigor três diplomas legais diferentes para regular aspectos parcelares da mesma realidade concreta. Esta trilogia, para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do CPP, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático[85]".

3. Incompatibilizações entre a Lei nº109/2009 e o CPP

3.1. Lei nº32/2008 e Lei nº109/2009 X Artigo 189º, CPP

O primeiro problema surgiu do facto de antes da recolha de prova digital ser regulada pela lei do cibercrime, foi regulada pelo CPP, conforme artigo 189º, que foi estendido[86] através da reforma de 2007 para abranger a recolha de prova eletrónica. Assim, segundo Carlos Pinho, "actualmente existem três regimes diversos de aquisição processual de dados de base, de tráfego e de localização: o regime processual penal geral, previsto no Código de Processo Penal e dois regimes especiais, o da Lei 32/2008, de 17 de julho e o da Lei 109/2009, de 15 de setembro (Lei do Cibercrime), todos com requisitos diversos e com

---

83 "Este direito protege toda a espécie de comunicação interpessoal, privada ou não, efectuada por intermédio da correspondência e das telecomunicações, independentemente do meio técnico utilizado e do seu conteúdo (...) O direito ao sigilo da correspondência e de outros meios de comunicação privada impede a sua violação ou devassa por terceiros ou pelo Estado, mas impõe também a proibição da sua divulgação, por aqueles que a ela tenham acesso, designadamente no exercício da sua profissão. Neste caso pressupõe a existência de um dever de sigilo profissional (...)", CORREIA, João, "Qual o significado de abusiva intromissão...", pp. 51-52.

84 "Em particular, dois desafios não poderiam deixar de ser enfrentados pela lei do cibercrime na adaptação da Convenção do Conselho da Europa: estabelecimento de parâmetros conforme a Constituição e clarificação da congruência e articulação da pluralidade de fontes normativas.", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 112.

85 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do MP,* nº139 (Julho-Set, 2014) p. 30.

86 "Sendo, então, o único regime processual penal sobre intercepções o legislador viu-se na necessidade de prever a extensão desse regime processual da intercepção e a gravação de conversações ou comunicações telefónicas em tempo real a outras realidades através de uma norma de extensão do regime – então no artigo 190º, agora no artigo 189º - a uma realidade diversa mas próxima do regime das comunicações telefónicas clássicas, isto é, 'as conversações e comunicações transmitidas por qualquer meio técnico diferente do telefone'", Cfr. Ac. TRE de 6-01-15, Processo nº: 6793/11.2TDLSB-A.E1, ponto B.3.2.

diversas estipulações e implicações relativamente às obrigações de conservação dos dados. A sua compatibilização prática depende de esforço interpretativo[87]".

Dessa forma, surgiu a dúvida sobre qual legislação aplicar nessa temática, dúvida esta que já foi sanada. Inclusive, há muitos acórdãos recentes do Tribunal da Relação[88] que deixam claro que no concernente à recolha de prova digital já não é mais aplicado o CPP, e sim a lei do cibercrime, devendo o art. 189º, nº1, CPP ser considerado parcialmente revogado de forma tácita pelo art. 18º, nº4, LCC, e o art. 189º, nº2 da mesma forma parcial e tacitamente revogado pelo art. 9º, nº1, lei 32/2008 no que tange a esta matéria. Já as incompatibilizações existentes entre a LCC e a lei 32/2008 serão posteriormente analisadas.

Segundo ac. TRE de 6-01-15, o artigo 189º, CPP foi parcialmente revogado por ainda estar em vigor no que se refere "às comunicações entre presentes e às comunicações não telefónicas que não impliquem a intervenção de qualquer 'sistema informático', se tal for possível[89]". Complementa, ainda, o ac. do TRE , de 6-01-15 que "as Leis nº 32/2008, de 17-07 e 109/2009, de 15-09 (Lei do Cibercrime) revogaram a extensão do regime das escutas telefónicas, previstos nos artigos 187º a 190º do CPP, às áreas das 'telecomunicações eletrónicas', 'crimes informáticos' e 'recolha de prova eletrónica[90]'".

No mesmo sentido está o acórdão do TRE de 20-01-15 que complementa que "esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por 'localização celular conservada' – uma forma de recolha de prova electrónica – desde a entrada em vigor da Lei 32/2008 (...). Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual 'geral' do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei nº109/2009, o do artigo 18º, nº1 do mesmo diploma a que corresponde um segundo

---

87 PINHO, Carlos, "Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho", *Revista do MP*, nº 129 (Jan-Mar 2012), p. 79.

88 Cfr. *Jurisprudência sobre prova digital, nota prática nº 6/2015*: Acórdãos do Tribunal da Relação de Évora de 6 de janeiro de 2015 e de 20 de janeiro de 2015: "o regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às 'telecomunicações eletrónicas', 'crimes informáticos' e 'recolha de prova eletrónica (informática)' desde a entrada em vigor da Lei do Cibercrime. Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal previsto nos artigos 11º a 19º da Lei do Cibercrime", disponível em: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_6_jurispridencia_processual.pdf, acedido a 16-03-19.

89 Ac. TRE de 6-01-15, ..., ponto B.5.

90 Ac. TRE de 06-01-15, ..., ponto 1.

regime processual de autorização e regulação probatória. Só a este segundo regime – o dos artigos 18º e 19º – são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do CPP e sob condição de não contrariarem a Lei 109/2009[91]", e desde que esteja em causa a intercepção de comunicações[92], o que demonstra a aplicação subsidiária[93] desses dispositivos legais do CPP. Nota-se que essa remissão expressa do artigo 18º, nº4, LCC, não incluiu o artigo 189º, CPP, que acabou por ter seu regime de extensão[94] substituído. Assim, o artigo 189º, CPP "nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável[95]".

Em compatibilidade com a jurisprudência, a doutrina[96] possui o mesmo posicionamento, conforme João Conde Correia que acertadamente determina que "do ponto de vista doutrinal parece claro, desde logo, que a Lei 32/2008 e, depois, a Lei 109/2009 revogaram tacitamente parcelas importantes do regime consagrado no artigo 189º do CPP, reduzindo muito o seu alargado âmbito de aplicação inicial. Essas leis extravagantes sobrepõem-se àquele regime geral, que só subsiste naquilo que não foi depois especialmente regulado[97]". No mesmo sentido dispõe Paulo Dá Mesquita que "o acesso, a intercepção, o registo e a recolha dos dados de conteúdo das telecomunicações electrónicas encontra-se regulada na lei do cibercrime, exceptuando o universo que continua subordinado ao regime da intercepção e gravação de conversações ou comunicações telefónicas[98]", o que invoca mais ume vez a revogação tácita e parcial do art. 189º, CPP.

Entretanto, em sentido contrário existe o posicionamento de Pedro Verdelho, que dispõe que "este regime especial (intercepção de comunicações) não revogou o previsto no art. 189º, CPP nem colide com o mesmo, limitando-se a criar um regime específico, de âmbito limitado aos crimes descritos na Lei do Cibercrime. Dessa forma, o regime do art.

---

91 Ac. TRE de 20-01-15, Processo nº 648/14.6GCFAR-A.E1, pontos 2 e 4.

92 Ac. TRE de 20-01-15, ..., ponto B.3.4.

93 *Idem*

94 *Idem*

95 Ac. do TRE de 6-01-15, ..., ponto B.3.5.

96 "(...) a lei do cibercrime não assumiu de forma expressa a alteração do artigo 189, nº1, do CPP, parcialmente revogado pela regulação mais completa e exaustiva dessa lei, o que se apresenta gerador de problemas dispensáveis ao nível da interpretação e, fundamentalmente, da aplicação do direito constituído", MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 102.

97 CORREIA, João Conde, "Prova digital: enquadramento legal", in *Ebook Cibercriminalidade e Prova Digital*, Centro de Estudos Judiciários, julho de 2018, p. 18.

98 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 123.

189º mantém-se em vigor para todos os restantes casos[99]". Paulo Pinto de Albuquerque[100] partilha dessa mesma opinião da qual discordamos.

Já Carlos Pinho[101] também acertadamente considera admissível a interpretação de que o artigo 189º, nº2, CPP foi tacitamente revogado pela lei 32/2008, por se encontrar em conformidade com a intenção do legislador ordinário (Assembleia da República), bem como pelo facto da lei especial 32/2008 ter regulado todas as matérias do regime geral do CPP, o que permite a ocorrência de uma revogação tácita (artigo 7º, nº2, Código Civil). No entanto, o mesmo autor destaca graves consequências de tal interpretação: os crimes graves previstos no artigo 187, nº1, alíneas a), d), f) e g), CPP, por não coincidirem com os crimes graves do artigo 2, nº1, al. g) da lei 32/2008, não seriam abrangidos pela possibilidade de terem seus dados de base, de tráfego e de localização conservados e transmitidos, conforme artigo 9º, nº1, lei 32/2008. Assim, "comprometer-se-ia de forma decisiva a realização da justiça e tornar-se-iam alguns destes crimes (designadamente os cometidos por meio de telefone) em verdadeira letra morta, com grave prejuízo para os cidadãos vítimas destes crimes[102]". A solução acertada proposta por Carlos Pinho[103] é de alteração do disposto no art. 2º, nº1, g), lei 32/2008, que deveria ter a seguinte redação: "crimes graves, os crimes previstos no nº1 do artigo 187º, CPP e na Lei nº 109/2009", como forma de compatibilizar os regimes e reestabelecer a coerência nesta temática.

Além do artigo 18º, nº4, LCC, há outros dispositivos nessa lei (artigos 14º, nº7; 15º, nº6; 16º, nºs 5, 6; 17º in fine e 19º, nº2) que fazem remissão a artigos do CPP, permitindo sua aplicação, mas de forma subsidiária, o que denota o caráter secundário[104] e dispensável das normas do CPP no que tange a matéria de recolha de prova digital, sendo a lei do cibercrime a que prevalece. Nesse sentido, dispõe acertadamente Militão que "todas as medidas, gerais ou excepcionais, e obrigações previstas na Lei nº 109/2009, cumulam-se ainda, em tudo o que não as contrarie, com as estabelecidas no CPP"[105]. Assim, outros meios

---

99 VERDELHO, Pedro, "A nova lei do Cibercrime", *Scientia Iuridica*, Tomo LVIII, nº 320, 2009, p. 747.

100 ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 4ª edição atualizada, 2011, p. 549.

101 PINHO, Carlos, "Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho", *Revista do MP*, nº 129 (Jan-Mar 2012), pp. 89-90.

102 PINHO, Carlos, "Os problemas interpretativos...", p. 91.

103 PINHO, Carlos, "Os problemas interpretativos...", pp. 92-93.

104 Ac. TRE de 20-01-15, ponto B.3.4.

105 MILITÃO, Renato Lopes, "*A propósito da prova digital*...", pg. 278.

de obtenção de prova previstos no CPP como a perícia[106] (art. 151º, CPP) e os exames (art. 171º, CPP), continuam a poder ser utilizados no que tange a recolha de prova em suporte digital. É o que estabelece João Correia ao afirmar que "em certas circunstâncias poderá, por exemplo, ser necessário proceder a uma perícia informática ou até, mesmo, examinar um computador. Aliás, a própria Lei do Cibercrime fala de 'pesquisa informática ou de outro acesso legítimo a um sistema informático' (arts. 16º e 17º) demonstrando que, afinal, aquela lei não detém o exclusivo na aquisição processual de dados informáticos. O legislador reconheceu a existência de outras formas, retornando, assim, ao Código de Processo Penal, que *ab initio* se quis afastar com a opção por um regime especial[107]". Já o artigo 189º, nºs 1 e 2, CPP não é mais aplicável, nem subsidiariamente, à obtenção de prova eletrónica por ter sido parcialmente revogado pelas leis 109/2009 e 32/2008.

O legislador teria evitado esse problema de compatibilização se ao invés de ter criado uma lei específica tivesse regulado no próprio CPP[108], com a revisão de 2007, normas especiais processuais relativas a temática da prova no cibercrime. Porém, conforme a exposição de motivos da proposta de lei do cibercrime, o legislador agiu corretamente[109] em criar um diploma novo ao invés de alterar e adaptar os já existentes pelo facto de já existir em matéria penal legislações avulsas[110] que regulam uma matéria específica, bem como pelo facto da "geral inconveniência de ver em diplomas estruturantes do ordenamento penal regras especiais, apenas aplicáveis a uma parcela muito restrita dos tipos de ilícito; por outro, a conveniência prática, para os operadores judiciários, de ver sistematizado todos os

---

106 Para maiores esclarecimentos sobre prova pericial e exames, consultar VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada,* Coimbra Editora, 2011, pp. 91-92.

107 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter"; *Revista do MP*, nº 139 (Julho-Set 2014), p. 50.

108 "Alteração envergonhada do Código de Processo Penal pela lei do Cibercrime" lhe chama Dá Mesquita, que afirma que o Capítulo III da Lei 109/2009, relativo às disposições processuais, deve ser encarado como um escondido Capítulo V (Da prova electrónica), do Título III (Meios de obtenção de prova) do Livro III (Da prova) do Código de Processo Penal", cfr. Ac. TRE de 20-01-15, ponto B.3.3 e MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 101.

109 "Esta opção minimalista do legislador – a de colocar no regime de extenção a regulação processual de matérias distintas – foi largamente criticada pela doutrina, por recusar um tratamento processual consistente do processo necessário às novas realidades das telecomunicações e da informática", cfr. Ac. do TRE de 20-01-15, ponto B.3.1.

110 "Afigura-se ser esta a opção legislativa mais coerente com a tradição portuguesa, onde existem, especificamente na área penal, outros diplomas estruturantes de matérias na especialidade: assim acontece com a criminalidade relacionada com estupefacientes, com os crimes contra a economia ou com a criminalidade fiscal, cujos quadros penais e processuais específicos estão definidos em diploma próprio", cfr. exposição de motivos da proposta de Lei nº 289/X/4ª, ..., p. 3.

normativos referentes a um sector específico da criminalidade[111]".

Há de se considerar o posicionamento acertado de Paulo Dá Mesquita, segundo o qual, esses três argumentos são frágeis, contraditórios e incompatíveis, já que "o argumento da tradição invocado na exposição de motivos é desmentido pela originalidade da Lei do Cibercrime em matéria de regras processuais (...) Com efeito, no caso das legislações mencionadas na exposição de motivos como ilustrando a tradição as normas processuais reportam-se apenas a regras especiais relativas aos tipos de crime consagrados nesses diplomas e não são aplicáveis genericamente a qualquer tipo de crime como as que surgem plasmadas na Lei do Cibercrime. Este aspecto, obviamente, inverte o terceiro dos argumentos da exposição de motivos, já que os normativos processuais em causa não se reportam 'a um setor específico da criminalidade', pelo que é da 'conveniência prática' dos operadores judiciários que os mesmos não estejam inseridos em legislação aparentemente dirigida apenas 'a um sector específico da criminalidade'. Quanto ao segundo argumento também cai pela base, pois o capítulo III da Lei do Cibercrime não prevê normas especiais em sentido técnico-jurídico, mas regras de obtenção de prova em suporte electrónico aplicáveis a um elenco de crimes mais amplo do que o dos crimes de tabela das escutas telefónicas[112]".

Assim, segundo Militão[113], como as normas relativas a recolha de prova digital elencadas na lei do cibercrime, conforme artigo 11º, lei 109/2009, são de aplicação geral, para vários tipos de crimes e não apenas para os encontrados na referida lei, essas normas deveriam ter sido inseridas no CPP em um novo capítulo[114], como meio de facilitar sua aplicação. Dessa forma, foi desnecessária a criação de uma nova lei, o que ainda veio a acarretar problemas de compatibilização com diplomas já existentes. Nesse mesmo sentido concordamos com João Conde Correia que dispõe que com "a publicação desta nova lei,

---

111 Exposição de motivos da proposta de Lei nº 289/X/4ª, ..., p. 3.

112 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p.99.

113 MILITÃO, Renato Lopes, "*A propósito da prova digital...,* p. 266.

114 "Em face do exposto, impunha-se a integração das regras no Código de Processo Penal, pois, para usar as mesmas expressões da exposição de motivos, essa seria 'a opção mais coerente com a tradição portuguesa', em face da 'geral inconveniência' de ver dispersas em leis extravagantes regras gerais carecidas de enquadramento no Código de Processo Penal enquanto 'diploma estruturante' e a 'conveniência prática, para os operadores judiciários, de aí ter sistematizados todos os normativos' que não são apenas aplicáveis 'a um setor especifico da criminalidade' no Código de Processo Penal (...) nada obsta a que o intérprete aborde o cap. III da Lei do Cibercrime essencialmente como um envergonhado ou escondido novo cap. V (da prova electrónica) (...) do Código de Processo Penal". MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p.101.

satisfazendo as obrigações internacionais do Estado Português, o legislador nacional consagrou, finalmente, um verdadeiro sistema processual de prova digital. Todavia, mais uma vez, a opção legislativa passou pela escolha da via lateral e acessória da legislação extravagante, em detrimento do aconselhável regime geral. Em vez de uma, as fontes da prova digital passaram, entre nós, a ser três... A coexistência formal destas três normas gera extensas zonas de confronto e de atrito, porventura impercetíveis ao observador menos atento[115]". Assim, sugere João Correia que "urge, por isso, recuperar a centralidade normativa do CPP, enquanto instrumento nevrálgico da perseguição criminal, reservando para a legislação especial aquilo que é acessório, técnico, excecional. Normas como as que preveem a prova digital, pela sua importância, pelos interesses que regulam, pelas consequências que desencadeiam e, até, pela frequência com que são utilizadas devem constar do CPP[116]".

3.2. Artigo 15º, Lei nº109/2009 X Artigo 174º, CPP

Em decorrência do art. 15º, nº6, LCC, aplica-se às pesquisas de dados informáticos, com as necessárias adaptações, as regras das execuções das buscas previstas nos artigos 174º e 251º, CPP.

Assim, superada aquela problemática, percebe-se que há uma outra existente entre a incompatibilidade do artigo 15º, nº3, al. a, LCC com o artigo 174º, nº5, al. b, CPP. Enquanto a lei do cibercrime permite que o órgão de polícia criminal realize a pesquisa de dados informáticos sem prévia autorização da autoridade judiciária quando "a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados", o CPP permite que o órgão de polícia criminal efetue revistas e buscas sem prévia autorização da autoridade judiciária em que os visados consintam.

Percebe-se que nem sempre quem detém a disponibilidade ou controlo desses dados é o visado. Assim, como proceder quando, por exemplo, for realizada uma busca em uma empresa, em que esta detém os dados mas não há o consentimento do visado? Poderão os órgãos de polícia criminal proceder às buscas sem despacho prévio? Não há jurisprudência[117]

---

115 CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 18.

116 CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 27.

117 "Não obstante, (...) e apesar da Lei do Cibercrime ter já nove anos, continua escassa a jurisprudência existente sobre algumas das questões, não sendo raro encontrar-se acórdãos de tribunais superiores que ignoram a sua existência", CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 51.

sobre essa questão que tem gerado discussão.

No entanto, João Correia[118] tem entendido que tratando-se de uma empresa e não de um computador pessoal[119], em princípio, pode o chefe da secção permitir o acesso aos dados do computador usado para trabalho pelos órgãos de polícia criminal sem necessidade de despacho prévio de autorização da autoridade judiciária ou consentimento do visado, desde que haja consentimento do chefe, detentor do controlo dos dados em questão. Esse posicionamento está em consonância com o facto já abordado na presente dissertação de que as disposições do CPP têm aplicação subsidiária com relação à lei do cibercrime (a que prevalece), sendo aplicadas apenas no que não a contrariarem. Entretanto, percebe-se que a reserva da intimidade e da vida privada do visado (art. 26º, nº1, CRP) ficam comprometidas, vulneráveis, desprotegidas, bem como a inviolabilidade e o sigilo das comunicações (art. 34º, nºs 1, 4, CRP).

Nesse sentido, ressalva acertadamente João Conde Correia que essa "solução facilita muito as funções das instâncias formais de controlo, mas desconsidera irremediavelmente a reserva da intimidade da vida privada do visado, admitindo que um terceiro possa permitir o acesso aos dados – sejam eles quais forem – ali guardados (...)[120]"; Ainda, segundo ele, "isso não significa que o computador não possa ser acedido (transformando-o numa espécie de território sagrado), mas apenas que deverá haver mais cuidado no seu acesso não legitimador por uma qualquer autorização legal válida[121]".

Já Benjamim Rodrigues possui uma interpretação restritiva do artigo 15º, LCC, ele entende "no sentido de se apagar a aparente abertura para que esta operação ocorra sem que à mesma presidia a autoridade judiciária que a ordenou ou autorizou. Mais. Julgamos que, por força do artigo 32º, nº4, CRP, esta autorização tem de ser judicial e, à semelhança do que ocorre com o 179º, nº3 do CPP, caberá ao juiz presidir a tal operação para que se mantenha a 'chain of custody', ou seja, a força probatória de tais elementos, sob pena de se desconsiderar a valoração dos mesmos em virtude de não darem garantias de autenticidade,

---

[118] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", pp. 50-52.

[119] "Tratando-se de um computador pessoal, quem tem disponibilidade sobre ele não terá, em princípio, legitimidade para autorizar a intromissão no seu conteúdo", já que "O computador funciona hoje, muitas vezes, como uma extensão da personalidade (...), podendo conter escritos, imagens, sons ou outros registos relativos ao núcleo intangível e absoluto da intimidade de cada um, pelo que só deverá poder decidir se os torna ou não públicos", CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 24.

[120] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 51.

[121] CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 24.

fidedignidade e não contaminação[122]".

Discordamos da disposição em sentido contrário de Duarte Rodrigues Nunes[123] que entende que apenas as lesões intensas devem ser autorizadas pelo juiz, e não toda e qualquer restrição de direitos fundamentais, já que de qualquer modo seria o juiz a avaliar se a lesão seria intensa ou não. Além disso, a CRP é clara e não determina que o juiz é obrigado a intervir apenas quando houver lesões intensas, mas quando estiver em causa direitos fundamentais, ou seja, ela não faz nenhuma distinção, não cabendo ao doutrinador fazê-la.

No que tange ao artigo 15º, nº3, al. a, LCC, Benjamim Rodrigues acertadamente entende que "há um perigo (...) de os agentes actuarem de forma desleal, no sentido de que já tendo uma suspeita minimamente fundada, relativamente a um suspeito, e que já seria suficiente para o constituir o arguido, se dirijam ao mesmo e de forma 'engenhosa, desleal e alguma artimanha' lhe solicitem dados que o irão autoincriminar sem o informarem de que lhe assiste o direito de prestar ou não a referida colaboração e que, por muito que seja, sempre existe um certo mínimo de perigo de a sua colaboração – consentimento – permitir o acesso a dados que doutro modo os órgãos nunca teriam acesso e, no entanto, serão fundamentais para a condenação do suspeito[124]". Assim, percebe-se que mais uma vez a lei do cibercrime deixa vulnerável os direitos fundamentais, neste caso, o direito à não autoincriminação do arguido, na sua vertente direito ao silêncio prevista no artigo 61º, nº1, al. d, CPP.

Problema semelhante e que carece de regulamentação legal ocorre quando o possuidor do computador for coercivamente obrigado a fornecer a palavra-passe (password) que dá acesso aos conteúdos do mesmo. Nesse sentido dispõe João Correia que "quando o notificado for o próprio arguido, não havendo entre nós nenhuma norma habilitante, dificilmente se poderão superar os constrangimentos processuais penais decorrentes do princípio *nemo tenetur se ipsum accusare*. O arguido não pode ser forçado a contribuir para a sua própria condenação. Ainda assim, não se tratando de um princípio absoluto, o legislador poderá criar situações circunscritas em que seja proporcional impor a colaboração do arguido (...). Quando o notificado for uma mera testemunha (situação menos provável, mas ainda possível) a solução será mais fácil. Excecionando os casos em que ele possa

[122] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 525.

[123] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime,* Gestlegal, 2018, p. 113.

[124] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 527.

validamente recusar-se a prestar declarações (arts. 132º, nº2 e 134º do CPP), a recusa em fornecer a password será ilegítima, podendo ser sancionada[125]".

Percebe-se que em ambas as situações, quando o visado (suspeito ou arguido) detiver o controlo ou a disponibilidade dos dados informáticos em causa ou da password que dê acesso a eles for induzido ou coagido a fornecer o acesso a essas informações, estará sendo violado o seu direito à não autoincriminação e de permanecer em silêncio. Muito embora esse direito não seja absoluto[126], por via do princípio da proporcionalidade (art. 18º, nº2, CRP) e ponderação de interesses, percebe-se que a intenção do legislador foi de salvaguardar esse direito em detrimento da eficácia da investigação criminal e a tutela da justiça, conforme dispõe o próprio art. 14º, nº 5, LCC, o que não poderia ser diferente no âmbito do art. 15º, LCC, apesar de não haver disposição expressa. Assim, deveria o legislador ter se preocupado em regular essa questão de modo a evitar a ocorrência de situações em que haja a violação desproporcional do direito à não autoincriminação. No entanto, segundo Rita Neves, "a recusa do arguido na revelação da palavra-passe não veda efetivamente o acesso aos dados informáticos, ao abrigo do *nemo tenetur*, apenas fazendo com que tenha que haver, mais tarde, um desbloqueio técnico da palavra-passe[127]".

E quando os dados informáticos ou a password a serem fornecidos estiverem sob o controlo ou disponibilidade de um terceiro (pode ser uma testemunha) este deverá fornecer as informações solicitadas com base na disposição da lei do cibercrime: ou voluntariamente sem despacho prévio do juiz ou involuntariamente após despacho do juiz, ou mesmo após uma coação ou induzimento que pode vir a ocorrer. Dessa forma, os direitos fundamentais do visado como a reserva da intimidade da vida privada, a inviolabilidade e o sigilo das comunicações ficam mais uma vez vulneráveis[128] pois permite-se que um terceiro disponha de dados que não lhe pertencem.

Assim, segundo os autores citados, a solução menos danosa aos direitos fundamentais seria a que não permitisse em nenhuma hipótese o acesso a dados informáticos ou a password de um computador sem uma autorização prévia do juiz, de acordo com o

---

125 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 59.

126 São exemplos de restrições por via da proporcionalidade os exames de alcoolémia e substâncias psicotrópicas ou os exames de ADN para fins de investigação criminal, NEVES, Rita Castanheira e CORREIA, Hélder Santos, "A Lei do Cibercrime e a colaboração do arguido no acesso aos dados informáticos", *Actualidad Jurídica Uría Menéndez,* nº 38, out. 2014, p. 146.

127 NEVES, Rita Castanheira e CORREIA, Hélder Santos, "A Lei do Cibercrime e a colaboração...", p. 149.

128 Nesse sentido dispõe NUNES, Duarte Rodrigues, *Os meios de obtenção de prova...,* pp. 94-95.

artigo 32º, nº4, CRP, que avaliaria a necessidade de tal medida, com base no artigo 18º, nº2, CRP. Evitar-se-ia, assim, a prática de coação e induzimento para com o visado e terceiros que detenham o controlo ou a disponibilidade das informações em questão.

3.3. Artigo 17º, Lei nº109/2009 X Artigo 179º, CPP

Outra questão que tem gerado discussão é entre o artigo 17º, lei 109/2009 e o artigo 179º, CPP[129]. O artigo 17º traz uma norma específica na lei do cibercrime sobre apreensão de correio eletrónico (meio de obtenção de prova que tem sido recorrentemente utilizado) ou registos de comunicação de natureza semelhante, que não havia na decisão quadro pelo facto dela não conter disposições processuais. Do mesmo modo, a Convenção do Cibercrime também não possui norma específica sobre apreensão de correio eletrónico, apesar de ter trazido disposições processuais no seu capítulo II. Assim, segundo constata Rui Cardoso, "a inspiração para o artigo 17º da LCC não está, pois, nem na Cciber, nem na Decisão-Quadro nº 2005/222/JAI. A origem deste artigo está apenas na proposta de Lei nº 289/X/4ª, tendo ela mesma exacta redacção que o artigo 19º desta[130]".

O problema surge quando o artigo 17º faz uma remissão para aplicação correspondente do regime da apreensão de correspondência do CPP, regulada nos artigos 179º e 252º. Porém, como o legislador não delimita o que deve ser aplicado correspondentemente, quem fará essa delimitação será o juiz no caso concreto, o que pode causar disposições contrárias entre ele e o MP, já que o MP quererá sempre que possível aceder aos dados, e o juiz deve intervir sempre que estiver em causa direitos fundamentais, dados pessoais, conforme artigo 32º, nº4, CRP.

Ao comparar o regime da lei do cibercrime sobre apreensão de correio eletrónico e o regime do CPP sobre apreensão de correspondência, percebe-se que há algumas incompatibilizações resultantes de omissões[131] por parte da lei do cibercrime. Enquanto o CPP

---

129 "...muito embora se disponha no enunciado do seu nº1 que é aplicável a 'qualquer outra correspondência', não nos parece que aquela inclua uma realidade virtual...", NEVES, Rita Castanheira, *As ingerências nas comunicações*..., p. 185. Discordamos desse entendimento, uma vez que a própria lei do cibercrime permite uma aplicação correspondente do regime da apreensão de correspondência do CPP, o que indica uma certa proximidade entre os sistemas.

130 CARDOSO, Rui, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei nº 109/2009, de 15.IX", *Ebook Centro de Estudos Judiciários*, julho de 2018, p. 52.

131 "(...) o legislador persiste em incompreensíveis omissões legislativas, criando lacunas inadmissíveis (...). Seja qual for a solução técnica adotada impõe-se, portanto, a atualização urgente da malha legislativa nacional, por forma a superar essas lacunas e a corrigir os estrangulamentos resultantes da incoerência de algumas

dispõe que deve-se tratar de crime punível com pena de prisão superior a três anos (artigo 179º, nº1, b), a lei do cibercrime nada diz; e enquanto o CPP regula que o juiz que autorizou ou ordenou a apreensão da correspondência deve ser o primeiro a tomar conhecimento do seu conteúdo (artigo 179º, nº3), a lei do cibercrime é omissa nesse ponto no que tange ao conteúdo dos e-mails. Além dessas questões, nenhum dos dois diplomas (art. 17º, LCC e 179º, nº1, CPP) deixa claro sobre a necessidade ou não de haver despacho judicial prévio a autorizar ou ordenar a recolha de mensagens por correio eletrónico ou apreensão de correspondência.

No que tange a primeira questão, percebe-se que grande parte dos tipos legais de crimes previstos na lei do cibercrime não têm moldura penal superior a três anos. Além disso, mesmo os artigos 18º e 19º, lei 109/2009 que preveem os meios de obtenção de prova mais intrusivos são aplicados aos crimes previstos na própria lei, independentemente da moldura penal. Assim, esse requisito do CPP para poder haver apreensão de correspondência não deve ser aplicado aos crimes da lei do cibercrime no que se refere a apreensão de correio eletrónico. Dessa forma, a apreensão de correio eletrónico também pode ser aplicada a qualquer crime, independentemente da sua moldura penal.

No que se refere à segunda questão, João Correia[132], em conformidade com Costa Andrade, Rita Castanheira Neves[133] e Pedro Verdelho[134], faz uma distinção entre e-mails lidos e não lidos, muito embora a lei do cibercrime não a faça, o que se relaciona com a distinção entre correspondência aberta e não aberta[135], conforme dispõe Rui Cardoso que "a correspondência merece tutela desde o momento do envio, fechada, até ao momento da abertura pelo destinatário. Como afirma Costa Andrade, 'é precisamente este facto – estar fechada – que define a fronteira da tutela penal do sigilo de correspondência e dos escritos, em geral'. Daí que, após aberta, a correspondência fique sujeita ao regime geral de apreensão, previsto no artigo 178º do CPP[136]".

---

soluções legais", conforme CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 56.

132 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 40.

133 NEVES, Rita Castanheira, *As ingerências nas comunicações*..., pp. 188-189.

134 Sobre este assunto, VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *Revista do MP*, nº 99, (Julho-Set 2004), p. 124.

135 "Não é juridicamente correcto, nem tecnicamente adequado, interpretar o art. 17º da forma diferente para mensagens abertas e mensagens não abertas", CARDOSO, Rui, "Apreensão de correio electrónico...", p. 63.

136 CARDOSO, Rui, "Apreensão de correio electrónico...", pp. 56-57.

Assim, o regime da proteção do sigilo da correspondência física do CPP só vale quando ela estiver em trânsito, quando ainda não foi aberta por seu destinatário. Isso porque, conforme João Correia "a partir desse momento (conclusão efetiva do processo de transmissão) o destinatário dispõe dos meios necessários a evitar a intromissão estadual. Ele já não está vulnerável, sujeito às falhas de reserva do operador ou à curiosidade estadual[137]". Da mesma forma, segundo Costa Andrade, "depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objecto idóneo da busca em sentido tradicional[138]".

No mesmo sentido, com relação aos correios eletrónicos, segundo João Correia[139], se eles já tiverem sido lidos, são considerados como meros documentos, devendo ser aplicado o artigo 16º, LCC (apreensão de dados informáticos) que facilita suas apreensões, já que bastaria a intervenção legitimadora do magistrado do MP. Já o artigo 17º, LCC (apreensão de correio eletrónico), que traz mais garantias, é aplicado se os e-mails não tiverem sido lidos. O artigo 18º, LCC (intercepção de comunicações) é aplicado aos e-mails em trânsito, ou seja, antes de chegarem ao servidor do destinatário. De forma semelhante, Paulo Dá Mesquita[140] defende uma interpretação restritiva do art. 17º, LCC, que seria aplicado apenas quando as transmissões das comunicações já foram processadas pelos fornecedores de serviços mas ainda não foram lidas, e o art. 18º, LCC quando ainda não foram transmitidas pelos fornecedores de serviços.

Porém, como os peritos informáticos demonstram que pode-se marcar facilmente uma mensagem como lida ou não lida, hoje em dia essa distinção entre correio eletrónico lido e não lido e as diferentes formas de tratamento defendidas por João Correia, Costa Andrade, Rita Neves, Pedro Verdelho e Paulo Dá Mesquita não fazem mais sentido[141]. Assim,

---

137 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 41.

138 ANDRADE, Manuel da Costa, "*Bruscamente no verão passado*", *a reforma do Código de Processo Penal,* Coimbra editora, 2009, p. 159.

139 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 41.

140 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 121.

141 "No que respeita às mensagens de correio electrónico ou registos de comunicações de natureza semelhantes, como veremos, é muito difícil ou mesmo impossível determinar quando é que terminou a comunicação e se a mensagem já foi ou não aberta/lida. Poderá, assim, não existir segredo de telecomunicações, porque estas

concordamos com Rui Cardoso que afirma que "alguns dos prestadores de serviço de correio eletrónico continuam a ter regimes de lido/não lido, mas que, contrariamente ao que sucede com a correspondência corpórea, podem ser facilmente alteráveis (e infinitamente) pelo utilizador, com um clique. O correio eletrónico pode ser arquivado pelo destinatário sem ser lido; pode ser arquivado juntamente com mensagens enviadas e até rascunhos de mensagens eventualmente a enviar[142]". Da mesma forma, hoje em dia as pessoas podem receber emails em diversos dispositivos, em uns pode constar como lido e em outros como não lido.

Assim, como esse critério de diferenciação não é seguro, deve ser descartado com relação aos correios eletrónicos, mas continua a fazer sentido no que tange as correspondências tradicionais. Dessa maneira, como não é possível saber se um e-mail foi de facto lido ou não, todos devem ter seu sigilo protegidos da mesma forma, com a aplicação mais garantística do artigo 17º, LCC. Já as correspondências físicas em trânsito, ainda não abertas pelo seu destinatário são tuteladas pelo artigo 179º, CPP, enquanto que as já abertas valem como um mero documento escrito, aplicando-se o regime geral de apreensão do artigo 178º, CPP.

Como a lei do cibercrime não é clara sobre o facto de dever ser ou não o juiz o primeiro a ter acesso ao conteúdo dos e-mails apreendidos, deve-se levar em consideração a análise da jurisprudência sobre o assunto no ac. do TRL de 11-01-2011 que determina que o regime geral do CPP sobre apreensão de correspondência deve ser aplicado "na sua totalidade, sem redução do seu âmbito" à apreensão de correio eletrónico, em conformidade com o que dispõe o art. 17º, in fine, LCC. Em contraposição, Rui Cardoso entende que "o art. 17º determina a correspondente aplicação do regime de apreensão de correspondência do CPP, não a aplicação integral. Esta só deve ser feita naquilo que não contrariar o já previsto na própria LCC; a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC. Como vimos, foi intenção do legislador adaptar às novas realidades a busca e a apreensão previstas no CPP, não aplicá-los integral e acriticamente[143]"

Considerando-se a posição do referido ac. TRL, o artigo 179º, nº3, CPP deve ter sua aplicação estendida ao conteúdo do correio eletrónico "já convertido em ficheiro legível, o que constitui acto da competência exclusiva do juiz de instrução criminal, nos termos do art.

---

podem já ter terminado; não existir segredo de correspondência, porque esta pode ter cessado com a abertura", CARDOSO, Rui, "Apreensão de correio electrónico...", p. 57.

[142] CARDOSO, Rui, "Apreensão de correio electrónico...", p. 63.

[143] CARDOSO, Rui, "Apreensão de correio electrónico...", p. 66.

268º, nº1, al. d, CPP, o qual estabelece que 'compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida', (...) constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova. A tudo isto acresce que a falta de exame da correspondência pelo juiz constitui uma nulidade prevista no art. 120º, nº2, al. d, CPP porque se trata de um acto processual legalmente obrigatório (neste sentido vide Paulo Pinto de Albuquerque, in comentário do CPP, 2ª edição, anotação 12ª ao art. 179º, pg. 495)[144]". Nesse sentido, concordamos que deve ser o juiz da instrução criminal que tiver autorizado ou ordenado a apreensão dos e-mails também o primeiro a tomar conhecimento do seu conteúdo, sob pena de nulidade e produção de prova proibida que não pode ser valorada.

Apesar disso, no próprio acórdão é feita uma ressalva apenas em caso de urgência, ou seja, "no caso de perda de informações úteis à investigação de um crime em caso de demora, o juiz pode sempre autorizar a abertura imediata de correspondência (assim como de correio eletrónico) pelo órgão de polícia criminal e o órgão de polícia criminal pode mesmo ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos nºs 2 e 3 do art. 252º, CPP, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja atempadamente convalidada, ou caso seja rejeitada a convalidação[145]".

Com base nessa decisão judicial, percebe-se que mesmo em situação excecional, caso de urgência, deve o juiz autorizar que o órgão de polícia criminal possa ler a correspondência antes dele, bem como deve convalidar por despacho fundamentado uma eventual ordem desse órgão de suspensão da remessa. Previsão semelhante existe nos artigos 15º, nº4, a, b, LCC e 16º, nº4, LCC. Essa participação do juiz destaca seu papel de protetor dos direitos fundamentais das pessoas, conforme artigo 32º, nº4, CRP, o que não poderia ser diferente no âmbito da cibercriminalidade, apreensão de correio eletrónico. Acórdão mais recente e em igual sentido é o ac. TRL de 6-02-2018[146], que reitera o posicionamento anterior, e indica que essa questão vem sendo decidida da mesma forma há anos pelo TRL.

Em sentido contrário, existe apenas o "acórdão do TRG de 29-03-2011, P. 735/10.0GAPTL-A.G1 (Maria José Nogueira), em que se considerou ser de aplicar à

---

144 Ac. TRL de 11-01-2011, Processo nº 5412/08.9TDLSB-A.L1-5, ponto 7.

145 *Idem*

146 Ac. TRL de 06-02-2018, Processo nº 1950/17.0T9LSB-A.L1-5.

apreensão de uma SMS o disposto no artigo 17º da LCC, mas podendo o Ministério Público aceder ao seu conteúdo antes da decisão de apreensão (formal) do juiz de instrução[147]".

Outro argumento existente é o do Procurador Rui Cardoso[148], que invoca a violação da estrutura acusatória do processo penal (art. 32º, nº5, CRP), já que ao se exigir que seja o juiz a ler os e-mails e a selecionar o que fica ou não no processo, seria ele a determinar as provas que ficam no processo, o que não seria função do juiz da instrução, mas do MP (titular do inquérito). Haveria, assim, usurpação de competências. No entanto, apesar de ser o MP o responsável pelas investigações e aparentemente o mais apto a decidir quais provas são mais relevantes para o processo, percebe-se que o juiz também deve ter amplo conhecimento da causa, sendo igualmente apto a realizar tal função. Além disso, o mesmo ocorre quando há a apreensão de correspondência tradicional do artigo 179º, CPP, já que a correspondência é dada ao juiz e é ele quem decide a prova que deve ou não ficar no processo, conforme artigo 179, nº3, CPP. No mesmo sentido, é o MP quem decide quais medidas de coação devem ser aplicadas (artigo 194º, nºs 1, 2, 3, CPP). Assim, entendemos que não há usurpação de competências, que estão delimitadas nas leis.

Dessa forma, não há impedimento para que seja o juiz da instrução o primeiro a ler o conteúdo dos e-mails apreendidos e a decidir o que fica ou não no processo, o que está em conformidade com a posição dominante dos acórdãos existentes sobre a matéria bem como com as disposições do CPP e o entendimento de Pedro Verdelho[149], que é mesmo anterior a publicação da lei do cibercrime. Caso contrário, poderia haver produção de prova proibida que não pode ser utilizada, bem como violação de direitos fundamentais. Esse entendimento também está em conformidade com o facto das normas do CPP deverem ter aplicação subsidiária com relação a lei do cibercrime, ou seja, podem ser aplicadas quando não contrariem a LCC bem quando esta for omissa na regulação de uma dada situação, como ocorreu no caso em questão.

No entanto, é importante destacar posicionamento em sentido contrário do próprio

---

147 CARDOSO, Rui, "Apreensão de correio electrónico...", p. 68.

148 CARDOSO, Rui, "Apreensão de correio electrónico...", p. 74.

149 "Se, ocasionalmente, na realização de uma diligência de investigação (busca ou exame a um computador), o órgão de polícia criminal que procede ao mesmo se aperceber da existência de mensagens de correio eletrónico com as mesmas características, não deverá aceder ao conteúdo dessas mensagens. Deverá apresentar o computador (...) ao Ministério Público, que o deverá apresentar ao juiz de instrução, para que este seja o primeiro a tomar conhecimento do correio", VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *Revista do MP*, nº 99, (Julho-Set 2004), pp. 123-124.

Pedro Verdelho[150] com relação a esta temática, já em obra posterior a publicação da lei do cibercrime. Mas, mesmo assim, ele destaca que a lei não foi clara nesse ponto. Segundo este autor, "estaria a optar-se por uma solução processual inviável, que exigiria a verificação, pelo juiz, de todas as mensagens de correio electrónico, em todos os computadores que fossem encontrados no decurso de pesquisas. Na verdade, esta solução seria inviável face à grande quantidade de computadores que nos dias de hoje se apreendem (...). Assim, não se exige que seja o juiz o primeiro a ter conhecimento de todas as mensagens (como acontece com o correio físico). A letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não[151]". Discordamos desse pensamento que está em conformidade com Duarte Rodrigues Nunes[152].

Se entendêssemos esse posicionamento de Pedro Verdelho como o mais adequado estaríamos a permitir que um número maior de pessoas (os realizadores das pesquisas) tivesse acesso a dados do visado, o que deixaria ainda mais vulnerável seus direitos fundamentais de sigilo das comunicações, bem como da reserva da intimidade de sua vida privada, contrariando-se o artigo 32º, nº4, CRP, que dispõe que o juiz pode delegar em outras entidades a prática de atos instrutórios desde que não se prendam diretamente com os direitos fundamentais. Da mesma forma, não faz sentido dizer que é inviável que o juiz dê conta de ser o primeiro a ler os vários e-mails, selecionando o é ou não relevante ao processo, mas que ele o possa fazer quando se trata de correio físico. Assim, como a regra do artigo 179º, nº3, CPP não contraria a lei do cibercrime, que é omissa nesta temática, pode e deve ser o juiz o primeiro a ter conhecimento do conteúdo dos correios eletrónicos apreendidos, o que está em conformidade com Rita Castanheira Neves[153].

No que tange a terceira problemática, ambos os diplomas dispõem que o juiz pode autorizar (o requerimento do MP no âmbito do inquérito) ou ordenar (quando há ordem do próprio juiz) por despacho a apreensão de correio eletrónico (LCC) ou apreensão de correspondência (CPP), mas não dizem se o despacho tem ou não que ser prévio.

O gabinete do cibercrime, mais precisamente, Pedro Verdelho[154], tem defendido que

---

150 VERDELHO, Pedro, "A nova lei do Cibercrime", *Scientia Iuridica*, Tomo LVIII, nº320, 2009, p. 744.
151 VERDELHO, Pedro, "A nova lei do Cibercrime...", p. 744.
152 NUNES, Duarte Rodrigues, *Os meios de obtenção de prova...,* p. 153.
153 NEVES, Rita Castanheira, *As ingerências nas comunicações...*, p. 275.
154 VERDELHO, Pedro, "A nova lei do Cibercrime...", pp. 743-744.

o MP e os órgãos de polícia criminal podem ordenar ou autorizar uma apreensão provisória ou cautelar das mensagens de correio eletrónico, que depois deverá ser submetida ao juiz e ser por ele validada (apenas nesse momento dá-se efetivamente a apreensão), não se exigindo que haja uma prévia decisão judicial para essa apreensão, posicionamento este que está de acordo com o já referido ac. TRG de 29-03-11. No entanto, entendemos que essa ideia de apreensão provisória não deve existir, deve haver despacho prévio do juiz da instrução. Isso pelo facto da lei dispor que o juiz pode autorizar ou ordenar, logo, a apreensão deve ser feita depois de haver despacho judicial.

Além disso, na prática, segundo Pedro Verdelho[155], quando uma busca é feita em uma casa ou em uma empresa, não se sabe se computadores serão encontrados, bem como em uma eventual pesquisa informática[156] não se sabe se e-mails serão encontrados, muito menos se os e-mails serão de interesse para a descoberta da verdade no que tange a prova. Assim, como forma de não ferir os direitos fundamentais das pessoas (reserva da intimidade da vida privada, artigo 26º, nº1, CRP), bem como a inviolabilidade e o sigilo da correspondência (artigo 34º, nº1, 4, CRP) deve haver despacho prévio do juiz, que deve avaliar se a apreensão (da correspondência ou do correio eletrónico) é ou não necessária para a descoberta da verdade, conforme artigo 32º, nº4 e 8, CRP e artigo 179º, nº1, c e nº3, CPP. Essa questão está em consonância com o facto de dever ser o juiz da instrução o primeiro a ler o conteúdo dos correios eletrónicos e registos de comunicações de natureza semelhantes apreendidos.

Mais uma vez destaca-se o posicionamento contrário de Pedro Verdelho antes da publicação da lei do cibercrime, que entendia que "se for previsível que, por exemplo, no decurso de uma busca, se irá encontrar, num computador, correio electrónico que se julga que irá ter interesse probatório, deve previamente suscitar-se junto do competente juiz de instrução a ordem de apreensão desse eventual correio[157]".

Nesse sentido dispõe João Correia que "parece haver alguma margem de constitucional para a implementação processual penal destas medidas. Segundo o BVerfG, a infiltração secreta em sistemas informáticos alheios, para efeitos de monitorização ou de leitura de dados, será constitucionalmente admissível, mediante prévia autorização judicial,

---

155 *Idem*

156 "A sua realização secreta, pelo contrário, retira ao visado qualquer possibilidade de controlo. Por falta de autorização legal expressa, as buscas online seriam assim inadmissíveis", conforme CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 44.

157 VERDELHO, Pedro, "A obtenção de prova...", p. 123.

em caso de perigo concreto para bens jurídicos individuais como a vida, o corpo ou a liberdade ou para interesses coletivos, cuja ameaça afete os fundamentos ou a sobrevivência do Estado de direito ou da própria existência humana[158]". Assim, consideramos que deve haver a extensão desse entendimento ao processo penal português, mais especificamente, no caso em questão, ao artigo 17º, LCC.

É importante salientar o que dispõem Gomes Canotilho e Vital Moreira no que se refere a extensão da aplicação do artigo 34º, CRP à correspondência eletrónica: "a garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o tráfego como tal (espécie, hora, duração, intensidade de utilização). No âmbito normativo do artigo 34º, cabe o chamado correio eletrónico, porque o segredo da correspondência abrange seguramente as correspondências mantidas por via das telecomunicações. O envio de mensagens eletrónicas de pessoa a pessoa (email) preenche os pressupostos da correspondência privada (Internet – serviço de comunicação privada)[159]".

Dessa forma, como já foi referido anteriormente, considerando ser o artigo 17º, LCC o mais protetor no que tange ao sigilo da apreensão de correio eletrónico em comparação com o artigo 16º, LCC que seria aplicado aos e-mails já lidos caso essa distinção fizesse sentido, percebe-se que mesmo esse artigo, menos protetor, no seu número 2, determina que os órgãos de polícia criminal só podem efetuar apreensões de dados informáticos sem autorização prévia da autoridade judiciária quando houver urgência ou perigo na demora, e mesmo essas apreensões sempre devem ser validadas pela autoridade judiciária (art. 16º, nº4, LCC). Nesse sentido, não poderia ser diferente a interpretação a ser dada ao artigo 17º, LCC, mais protetor, o que indica que a contrário *sensu*, quando não houver urgência, em uma situação normal, não pode haver apreensão de correio eletrónico e registos de comunicação de natureza semelhante sem despacho prévio de autorização ou ordenação do juiz competente, sendo esta a interpretação mais protetora possível dos direitos fundamentais das pessoas, principalmente a reserva da intimidade da vida privada e a inviolabilidade e o sigilo das comunicações, todos amparados constitucionalmente nos artigos 26º, nº1, 34º e 18º, CRP.

---

[158] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 44.

[159] CANOTILHO, Gomes, MOREIRA, Vital, *Constituição da República Portuguesa Anotada...*, p. 544.

4. Incompatibilizações entre a Lei nº109/2009 e a Lei nº32/2008

Com a entrada em vigor da lei do cibercrime, a mesma também acabou por ser incompatível em alguns aspetos com a lei 32/2008.

O artigo 11º, LCC trata do âmbito de aplicação das disposições processuais, ou seja, diz em que processos podem ser aplicados os meios de recolha e preservação de provas regulados na lei do cibercrime. O nº1, alínea a dispõe que os meios de obtenção e conservação de provas previstos na lei do cibercrime, com exceção dos artigos 18º (intercepção de comunicações) e 19º (ações encobertas), LCC, pelo facto deles preverem os meios de obtenção de provas mais intrusivos, mais violadores dos direitos das pessoas são aplicados aos crimes previstos na própria lei (regulados do artigo 3º ao 8º); bem como são aplicados a outros crimes previstos em outras leis, desde que cometidos por meio de um sistema informático (alínea b), como injúria, burla e difamação informáticas[160], por exemplo, ou a todos os crimes, em qualquer processo, desde que seja necessário proceder à recolha de prova em suporte eletrónico (alínea c)[161]. Assim, percebe-se que o âmbito de aplicação dos artigos 18º e 19º, LCC é menor em comparação aos demais meios de recolha e conservação de prova digital.

No que tange a esta alínea c, por ser regra de aplicação geral, o legislador deveria tê-la inserido não em legislação avulsa (lei do cibercrime), mas no capítulo relativo à prova no CPP, em uma seção relativa a recolha de prova em suporte eletrónico, como forma de facilitar sua aplicação a qualquer crime que necessite da obtenção de prova digital.

Um dos problemas de compatibilização entre ambos os diplomas legais decorre do que dispõe o artigo 11º, nº2, lei do cibercrime: "as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei nº 32/2008, de 17 de julho". Assim, como

---

160 "Esta amplíssima previsão abrange – seja pela al. b), seja pela al. c) do preceito – crimes habitualmente tidos como excluídos pela jurisprudência da possibilidade de prova, como por exemplo os crimes de difamação cometidos na internet que, abertamente, passam a ser de muito mais fácil investigação e prova", Ac. TRE de 20-01-15, ponto B.3.3.

161 "Ou seja, é amplíssimo o catálogo de crimes que cabem na previsão das alíneas b) e c) do nº1 do artigo 11º, principalmente nesta última e todos os crimes em que se revele a necessidade de fazer prova por recolha em suporte electrónico estão nela contidos (...) E a pretensão do legislador é o de, declaradamente, alargar o âmbito de aplicação da lei até onde haja necessidade de fazer prova (...)", Ac. TRE de 20-01-15, ponto B.3.3.

interpretar o termo "não prejudicam"[162]? Há decisões[163] que entendem que em tudo que não for compatível deve-se considerar que a lei do cibercrime de 2009 revogou tacitamente a lei 32/2008, muito embora o "objeto de ambas as leis seja parcialmente coincidente"[164]. Isso porque, segundo Carlos Pinho, "não sendo a remição efectuada para qualquer disposição específica, mas para a globalidade do regime contido na Lei nº 32/2008, a consequência seria a de não poderem sequer ser obtidos dados de base, de tráfego e de localização para as investigações relativas aos próprios crimes de catálogo da Lei do Cibercrime (salvo nas formas agravadas de sabotagem informática), porquanto se não inserem no conceito de crime grave previsto na alínea g) do nº1 do artigo 2º da referida Lei nº 32/2008[165]", uma vez que o artigo 9º dessa lei só permite a transmissão de dados das categorias conservadas no seu artigo 4º no que tange a descoberta da verdade e repressão de crimes graves.

Assim, dispõe o ac. TRE de 20-01-15 que "devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nºs 1 e 2 e o artigo 9º mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, nº1, Lei nº 32/2008 ou seja, dados conservados em geral. Revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, nº1, Lei 32/2008[166]". Dessa forma, percebe-se que como a lei do cibercrime é de aplicação geral, revoga tacitamente a Lei 32/2008 nos pontos em que esta também o for, mas não no que tange as suas disposições específicas[167], como os dados conservados relativos à localização celular. Da mesma forma dispõe o ac. TRE de 6-01-15: "como a harmonização das duas leis não é possível, entendemos, com a primeira das

---

[162] "Mas haverá que interpretar o nº2 do artigo 11 da Lei de 2009 e atribuir um sentido à expressão 'as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei nº 32/2008' face à criação de um regime 'especial' processual penal criado pelo diploma de 2009. Admitindo que o diploma de 2008 está em vigor na parte 'arquivística', que sem dúvida está, o que concretamente se deve apurar é se os artigos 3º, nº1 e 9º, nº 1 e 3 da citada Lei – o regime processual de acesso a dados de localização conservados – foram revogados pelo regime processual penal para dados informáticos, contido nos artigos 11º a 19º da Lei nº 109/2009", Ac. TRE de 20-01-15, ponto B.4.2.

[163] "Como a harmonização dos sistemas processuais das duas leis não é possível entendemos que a Lei nº 109/2009 revogou a Lei nº 32/2008 em tudo o que não seja a regulação da parte 'arquivística' do diploma e que não diga respeito aos dados contidos no seu artigo 4º", Ac. TRE de 20-01-15, ponto B.4.3.

[164] Ac. TRE de 20-01-15, ponto B.4.3.

[165] PINHO, Carlos, "Os problemas interpretativos...", p. 88.

[166] Ac. TRE de 20-01-15, ponto B.4.3.

[167] "(...) o regime 'geral' de prova electrónica é constituído pelos artigos 11º a 17º da Lei nº 109/2009 e apenas se aplicarão os dispositivos da Lei nº 32/2008 – artigos 3º e 9º - na medida em que estes são aplicáveis aos dados informáticos pretendidos. Mas no que não esteja especificamente previsto por tais preceitos aplicar-se-á o dito regime geral da lei do Cibercrime de 2009". Ac. TRE de 20-01-15, ponto B.4.3.

indicadas teses, que a Lei nº 109/2009 revogou a Lei nº 32/2008 em tudo que não seja a regulação da parte 'arquivística' do diploma. Assim, deve afirmar-se que o actual significado de certos preceitos desta lei se reduz ao seu sentido arquivístico[168]".

Nesse mesmo sentido dispõem Duarte Rodrigues Nunes[169] e Paulo Dá Mesquita, sendo que este entende que "no que concerne ao art. 9º da Lei nº 32/2008, relativo a transmissão de uma panóplia de dados que não são de conteúdo, o complexo normativo derivado da conjugação dos arts. 11º, 12º, 13º, 14º, 16º e 18º da lei do cibercrime determina a revogação do essencial daquele regime. Subsistindo a importância da Lei nº 32/2008, sobretudo, no estabelecimento dos deveres dos fornecedores de serviços de conservação e protecção desses dados, bem como das condições técnicas operativas e destruição desses dados[170]".

Já o entendimento predominante na doutrina portuguesa é no sentido de que não prejudicar significa tentar compatibilizar ambos os regimes[171], conforme dispõe João Conde Correia que "segundo a tese minoritária, a LCC revogou o regime de acesso àqueles dados subsistindo a lei nº 32/2008, sobretudo no que concerne ao 'estabelecimento dos deveres dos fornecedores de serviços e prestação desses dados (...). Aquela lei só sobrevive naquilo que não foi expressamente regulado pela LCC. Não há nenhuma razão para manter regimes diversificados de acesso e que, contraditoriamente, oneram a investigação dos crimes mais graves com exigências injustificadas. Em sentido contrário, a tese maioritária advoga que a relação será antes de pura complementaridade"[172]. Dessa forma, dispõe Carlos Pinho que ao se considerar que a lei do cibercrime revogou tacitamente a lei 32/2008 em tudo o que esta for com ela incompatível, "tal interpretação violaria determinantemente a intencionalidade da concordância prática entre os regimes a transpor pretendida pelo legislador comunitário, desde logo no estabelecimento de uma obrigação de preservação de dados às operadoras de serviços de comunicação para efeitos, designadamente, de investigação criminal[173]".

---

168 TRE de 06-01-15, Processo 6793/11.2TDLSB-A.E1, ponto B.3.5.

169 NUNES, Duarte Rodrigues, *Os meios de obtenção de prova...,* pp. 25-32.

170 MESQUITA, Paulo Dá, "Prolegómenos sobre prova electrónica...", p. 123.

171 "Naturalmente que sempre restaria resolver as contradições aparentes existentes entre as Leis 32/2008 e 109/2009, sendo aqui de realçar as duas correntes doutrinais que se entrechocam, a da revogação da primeira Lei pela segunda, deixando àquela, apenas, a regulação do acesso por via dos deveres dos fornecedores de serviços e a tese da co-habitação de ambas as leis na harmonia possível", Ac. TRE de 6-01-15, ponto B.3.5.

172 CORREIA, João Conde, "Prova digital: enquadramento legal...", p. 18.

173 PINHO, Carlos, "Os problemas interpretativos...", p. 89.

Assim, tendo em consideração o posicionamento da doutrina maioritária, bem como a intenção do legislador, o mais adequado seria tentar compatibilizar ambos os diplomas em prol do objetivo maior, qual seja, de facilitar a investigação, a produção de provas e combater a cibercriminalidade. Em suma, segundo João Correia, "a legislação contida no Código de Processo Penal foi, no essencial, ultrapassada pelas Leis nºs 32/2008 e 109/2009, intercedendo entre estas duas – segundo a maioria – uma relação de pura complementaridade. O terceto reduziu-se afinal, pelo menos, a um simples dueto. Em cada situação concreta, o julgador deverá pois – num dispensável exercício de verdadeiro equilibrismo jurídico – verificar qual o regime processual aplicável, partindo depois para sua interpretação[174]". Entendemos mais uma vez que esse problema teria sido evitado se o legislador tivesse optado por regular a matéria da prova digital no regime geral do CPP e não em diversas legislações específicas.

Outro problema de compatibilização entre os dois diplomas legais dá-se entre o artigo 12º, lei 109/2009 e o artigo 6º, lei 32/2008. O artigo 12º (preservação expedita de dados), nº1 permite que certos dados informáticos (inclusive os de tráfego) necessários à produção de prova sejam preservados pelos fornecedores de serviço, no caso de se querer ter acesso a eles no futuro, por ordem da autoridade judiciária competente (MP ou juiz) por um período de no máximo três meses (nº3, al. c), podendo a autoridade judiciária ordenar a renovação da medida por sucessivos períodos de três meses até ser alcançado o limite máximo de um ano (nº5).

Já o artigo 6º, lei 32/2008 determina que os dados em causa, previstos no artigo 4º, nº1 da mesma lei, devem ser conservados pelo período de um ano pelos fornecedores de serviços a contar da data da conclusão da comunicação. No entanto, segundo artigo 3º, nº1 e 9º, nº1, lei 32/2008, essa conservação e transmissão de dados só pode ocorrer quando o objetivo for a investigação, detecção e repressão de crimes graves (definidos no art. 2º, nº1, al.g), requisito este que não existe na lei do cibercrime.

Assim, com a conjugação de ambos os dispositivos percebe-se que, por imposição legal, os fornecedores de serviços preservam os dados por até um ano. Nesse sentido dispõe Benjamim Rodrigues que "importa notar que o período máximo de três meses não deve ser ultrapassado, não sendo – a nosso ver – de discutir a possibilidade de renovação, à

[174] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 37.

semelhança do que ocorre com as escutas telefónicas, mas haverá que atentar ao prazo absoluto de conservação dos dados gerados e tratados no âmbito das comunicações electrónicas, disposto no artigo 6º, Lei 32/2008: um ano. Não admira, por isso, que a renovação da medida, nos termos do artigo 12º, nº5, possa ocorrer, mediante ordenação ou autorização da autoridade competente, por períodos de três meses, mas até um máximo inultrapassável de um ano. Portanto, teoricamente, a medida pode ser renovada por três vezes, por períodos máximos parcelares de 3 meses[175]". De acordo com este posicionamento está Pedro Venâncio[176].

No entanto, o problema de compatibilização surge quando a ordem de preservação do MP ou do juiz da instrução for dada no limite do prazo legal de um ano. Assim, conforme o artigo 6º, lei 32/2008 o prazo já teria expirado, mas segundo o artigo 12º, nº3, al. c e nº5, lei 109/2009 o prazo começaria a correr. *Quid iuris*?

Segundo Pedro Venâncio, "o regime jurídico aplicável à preservação de dados electrónicos resultará da conjugação das disposições processuais da LCC com as regras resultantes quer da Lei nº 32/2008, de 17 de Julho, quer da Lei nº 41/2004, de 18 de agosto, relativa à protecção de dados pessoais no âmbito das comunicações electrónicas[177]".

Assim, com a conjugação de ambos os diplomas em causa, verifica-se que, na prática, os dados podem ficar preservados por mais um ano, na medida em que a ordem de preservação da lei 109/2009 é no âmbito de investigação, de produção de provas com relação a um crime concreto que não tem de ser grave (tal como ocorre na lei 32/2008, artigo 3º, nº1), e vale apenas para o processo no qual ela foi dada. Percebe-se que o âmbito de aplicação é diferente do da lei 32/2008, conforme o entendimento de Duarte Rodrigues Nunes[178].

Nesse sentido, dispõe o gabinete do cibercrime que "esta possibilidade legal, que é expedita, é particularmente útil quando a investigação se apercebe de que o prazo de conservação de dados está próximo do seu termo[179]". Dessa forma, pensamos que esse entendimento é perigoso e prejudicial aos direitos fundamentais (sigilo das comunicações e

---

175 RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 522.

176 VENÂNCIO, Pedro Dias, *Lei do Cibercrime*..., p. 101.

177 VENÂNCIO, Pedro Dias, *Lei do Cibercrime*..., p. 101.

178 NUNES, Duarte Rodrigues, *Os meios de obtenção de prova*..., p. 50.

179 Pedidos de dados a operadores de comunicações, *Nota prática nº 8/2016*, de 18 de fevereiro de 2016, ponto 8, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp.pdf > consultado em 15-04-19.

reserva da intimidade da vida privada) dos envolvidos no caso, uma vez que seus dados podem ser preservados por mais um ano quando o magistrado ordenar a sua conservação no limite do prazo legal ao entender que há receio de que os dados sejam perdidos, alterados ou deixem de estar disponíveis, o que também pode ser usado como "manobra" judicial para se ganhar tempo, sendo utilizado em momento oportuno, ficando os dados dos envolvidos vulneráveis por mais tempo.

5. Problemas interpretativos invocados pela Lei nº109/2009

5.1. Artigo 12º, LCC

Além dos problemas de compatibilização com outros diplomas já analisados, percebe-se que a lei do cibercrime também invoca problemas interpretativos e alguns deles serão aqui apresentados.

Segundo Benjamim Rodrigues, o artigo 12º, nº1, LCC invoca uma grande imperfeição que pode causar graves problemas interpretativos, uma vez que prevê uma medida danosa aos direitos fundamentais (preservação expedita de dados) que pode ser aplicada para a produção de prova, em busca da verdade, "no decurso do processo". Assim, segundo aquele autor, deve-se entender que "a medida se limita ao processo penal e não a outros meios, já que ingerência é gravosa e, contendendo com 'meios de comunicação privada', somente poderá ser adoptada no âmbito de um 'processo criminal em curso', não valendo para outros tipos de processos como sejam o disciplinar ou desportivo[180]".

Da mesma forma que o artigo 12º, nº1, LCC percebe-se que os artigos 14º, nº1, LCC e 15º, nº1, LCC também preveem "no decurso do processo", sem deixar claro que se refere ao processo criminal em curso. Mesmo o artigo 11º, LCC que prevê o âmbito de aplicação das disposições processuais da lei do cibercrime, bem como o artigo 18º[181], nºs 1, 2, LCC, podem deixar margem para uma duplo entendimento.

Em sentido contrário, dispõe Pedro Venâncio: "Não concordamos com este autor quando este apelida de 'imperfeição gritante' a referência no nº1 do artigo 12º da LCC: '*se no decurso do processo for necessário à produção de prova'* sem expressa delimitação ao

[180] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 521.

[181] "Há que se notar que a intercepção e o registo de transmissão de dados informáticos somente podem ser autorizados durante o inquérito – o que pressupõe a sua inscrição num processo criminal 'em curso' – e não em acções preventivas ou proactivas de investigação criminal (...)", RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 532.

processo criminal. Parece-nos despicienda essa referência porquanto o âmbito de aplicação desta norma está taxativamente consagrada no artigo 11º da LCC que a reserva para 'a processos relativos a crimes' sendo por isso claro que esta medida, como as demais medidas consagradas nos artigos 12º a 17º, não são admissíveis 'noutros tipo de processo como o sejam o disciplinar ou desportivo[182]".

Assim, muito embora esteja subentendido que a interpretação a ser adotada seja a de que os artigos em causa se referem ao processo criminal em curso, o legislador deveria ter sido claro de modo a impedir interpretações diversas da que foi pretendida, bem como evitar que essas medidas de recolha e conservação de prova digital prejudiciais aos direitos fundamentais das pessoas possam ser aplicadas fora do processo penal em curso.

5.2. Artigo 14º, LCC

O artigo 14º, LCC permite que a autoridade judiciária competente (juiz ou MP) ordene que os detentores de certos dados informáticos específicos e determinados os comuniquem ao processo ou que permitam seu acesso para que seja possível a produção de prova necessária à descoberta da verdade. Essa ordem que facilita o acesso aos dados pode ser dirigida aos fornecedores de serviços (artigo 14º, nº4), mas não pode ser aos suspeitos ou arguidos no processo (artigo 14º, nº5), devido ao princípio da proibição da autoincriminação, sendo uma de suas vertentes o direito ao silêncio que tem previsão legal no artigo 61º, nº1, d, CPP. Da mesma forma, profissionais relacionados a área de jornalismo, advocacia, actividade médica e bancária não podem ser alvo de injunções para se permitir acesso aos dados armazenados em seus sistemas informáticos, em decorrência do segredo profissional (artigo 14º, nº 6 e 7). Nesse sentido, dispõe Benjamim Rodrigues, "tudo isto em nome dos valores ligados ao direito de defesa ou plenitude das garantias de defesa processuais penais, à privacidade ou reserva da intimidade ligada à saúde e que implica o sigilo dos dados 'sensíveis' da saúde das pessoas, o sigilo bancário e o sigilo profissional do jornalista e a respectiva liberdade de informação e expressão implicadas, todos direitos com assento constitucional, nomeadamente, nos artigos 26º, 34º, 35º, 37º e 64º, CRP 1976"[183].

É o artigo 14º, nº 4, alíneas a, b e c que indicam os dados que os fornecedores de serviços são obrigados a comunicar ao processo em decorrência da ordem da autoridade

[182] VENÂNCIO, Pedro Dias, *Lei do Cibercrime...,* p. 102.
[183] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", p. 524.

competente. Dentre eles, está inserido na alínea b (qualquer outro número de acesso) o endereço IP (internet protocol)[184], que é o código gerado quando o computador se liga a uma rede de internet. A problemática[185] desse artigo envolve justamente o endereço IP, cuja discussão é saber se se trata de um dado de base ou um dado de tráfego, o que tem implicações sobre quem pode dar ordem para se obter esse dado. Se for considerado dado de tráfego, a autoridade competente é o juiz da instrução, mas se for dado de base, a autoridade competente pode ser além do juiz da instrução, o MP. Essa questão surge em decorrência do artigo 32º, nº4, CRP que dispõe que "toda a instrução é da competência de um juiz, o qual pode, nos termos da lei, delegar noutras entidades a prática dos atos instrutórios que se não prendam diretamente com os direitos fundamentais". Assim, tratando-se de direitos fundamentais das pessoas (como os dados de tráfego) apenas pode o juiz da instrução intervir.

O gabinete do cibercrime dispõe que "na nota prática nº2/2013 (de 3 de abril de 2013) concluía-se que a jurisprudência dominante sustentava que o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, não devia ser submetido ao regime dos dados de tráfego, por se entender que este pedido não se refere a informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Por isso, concluía-se que pertencia ao Ministério Público a competência para pedir, a um operador de comunicações, a identificação do seu cliente que utilizou um determinado endereço IP num determinado dia e hora[186]".

Na sequência, o gabinete do cibercrime[187] elenca uma série de acórdãos posteriores à

---

184 "Quando um indivíduo está plugado na rede, são-lhe necessários apenas dois elementos identificadores: o endereço da máquina que envia as informações à Internet e o endereço da máquina que recebe tais dados. Esses endereços são chamados de IP – *Internet Protocol,* sendo representados por números, que, segundo LESSIG, não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos", MILITÃO, Renato Lopes, "*A propósito da prova digital...",* p. 264.

185 "A classificação do internet protocol (IP) como um dado de base, acessível pelo Ministério Público ou antes como um dado de tráfego, na disponibilidade exclusiva do juiz de instrução criminal é, igualmente um indesejável motivo de discórdia e de ineficácia. O elemento gramatical permite ambas as interpretações, gerando uma ampla margem de insegurança jurídica", CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 48.

186 Jurisprudência sobre prova digital, *Nota prática nº 6/2015*, de 27 de agosto de 2015, pg. 4, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_6_jurispridencia_processual.pdf > consultado em 2-04-19.

187 Jurisprudência sobre prova digital, *Nota prática nº 12/2017*, de 2 de novembro de 2017, pp 8-10, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_12_jurisprudencia_prova_digital.pdf > acedido a 15-04-19.

emissão daquela nota prática que confirmam o posicionamento dos tribunais no sentido de que o endereço IP deve ser tratado pelo regime de dado de base e não de tráfego[188], já que não indica a identidade da pessoa que utilizou o computador em dado momento. Assim, tem entendido os tribunais que pode ser o próprio MP a pedir o acesso ao endereço IP, não precisa ser o juiz.

Nesse sentido, o TRL de 18-01-2011 dispõe que "a identificação completa, morada e endereço de correio eletrónico do titular de determinado blog, bem como o IP de criação desse blog e o IP onde foi efetuado determinado post, constituem dados de base[189]"; A mesma decisão foi proferida no acórdão do TRL de 19-06-2014: "registos de IP identificados pelas supra mencionadas entidades ulteriormente veiculadas nos autos (...) não são dados de tráfego, mas antes 'dados de base' de comunicações electrónicas. Assim sendo, a obtenção destes dados informáticos não depende de autorização judicial por caberem na previsão do art. 18 da LCC. Com efeito, os 'dados de base' podem ser obtidos por via de injunção nos termos do art. 14 da LCC sendo tal injunção da competência do MP (...). Os dados obtidos pelo MP em sede de inquérito foram validamente obtidos por não pertencerem ao conjunto de dados que impõe a intervenção de juiz de instrução, uma vez que se não traduzem na obtenção de conteúdos da comunicação[190]".

Nesse mesmo sentido, defendendo que o IP é dado de base e não de tráfego, dispõe João Correia: "a ligação à rede não significa pois, necessariamente *communicatio*. Assim, parece inquestionável que o IP só deverá convocar a alargada tutela do sigilo das telecomunicações quando tiver subjacente, pelo menos, uma efetiva tentativa de comunicação[191]".

É importante salientar que a lei do cibercrime trouxe em seu artigo 2º, als. b e c uma nova definição de dados de tráfego[192], que difere da lei anterior, lei 41/2004, art. 2º, al. d, que trata da protecção de dados pessoais e privacidade nas telecomunicações, o que vem a

---

188 "Assim, apesar de este tipo de informação ser tecnicamente agrupado na informação referente a tráfego, o regime jurídico da sua obtenção é o mesmo dos chamados dados de base (modernamente referidos como dados relativos aos clientes)", conforme dispõe Pedido de dados a operadores de comunicações, *Nota prática nº 8/2016,* ..., ponto 4 > consultado em 15-04-19. Esse entendimento demonstra que pouco importa ser o IP dado de base ou de tráfego, uma vez que o tratamento dado a ele será o de dado de base.

189 Jurisprudência sobre prova digital, *Nota prática nº 6/2015*,..., p. 6, > consultado em 2-04-19.

190 Ac. do TRL de 19-06-14, Processo nº 1695/09.5PJLSB.L1-9.

191 CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter...", p. 48.

192 Sobre essa diferença, consultar VENÂNCIO, Pedro Dias, *Lei do Cibercrime*..., p. 99.

ocasionar mais um problema interpretativo, de compatibilidade entre essas leis. Segundo Pedro Verdelho[193] "uma interpretação livre e alargada do conceito de dados de tráfego presente na Lei nº 41/2004 quase poderia levar a incluir nele dados de conteúdo, o que, à luz dos conceitos constitucionais, inviabilizaria a sua utilização nos moldes previstos na Lei do Cibercrime". Assim, deve prevalecer o sentido disposto na lei do cibercrime.

Já o conceito de dados de localização, que não é tratado na lei do cibercrime, deve ser entendido conforme dispõe artigo 2º, al. e, Lei nº 41/2004. No entanto, ainda segundo Pedro Verdelho, "não se diz que os operadores devem preservar a sua confidencialidade nem se impõe a sua destruição. Pode, portanto, concluir-se que os dados de localização não têm a mesma protecção que os restantes dados referidos (o conteúdo das telecomunicações e os dados de tráfego), não estando desde logo cobertos pelo sigilo das telecomunicações[194]", o que demonstra que mais uma vez a lei do cibercrime deixou vulnerável a proteção dos direitos fundamentais das pessoas, sendo este consagrado no artigo 34, nº1, CRP.

Apesar dessa consideração acertada no que diz respeito à lei do cibercrime, não podemos esquecer que a Lei nº 32/2008 prevê em seu artigo 4º uma categoria de dados a conservar e em seu artigo 6º o período de conservação desses dados, englobando em seu artigo 2º, nº1, al. a os dados de localização. Assim, percebe-se que os dados de localização não foram completamente esquecidos, mas deveriam ter sido também regulados e protegidos pela lei do cibercrime.

5.3. Artigo 15º, LCC

Percebe-se que há uma grande lacuna no artigo 15º, nº2, LCC, já que ele prevê que o prazo máximo de validade do despacho da autoridade judiciária competente para que se proceda a pesquisa de dados informáticos é de trinta dias, sob pena de nulidade. No entanto, o artigo não deixa claro quando que esse prazo começa a ser contado. Assim, segundo Benjamim Rodrigues, "a autoridade judiciária deve indicar no acto autorizativo em que momento se deve iniciar a contagem para se evitar os tais 'cheques em branco' que vulgarmente ocorre, já que o órgão de polícia guarda, no bolso, a autorização judicial e executá-la-ia, a coberto de razões de ordem técnica ou tácita, para um momento oportuno,

[193] VERDELHO, Pedro, "A nova Lei do Cibercrime...", pp. 721-722.
[194] VERDELHO, Pedro, "A nova Lei do Cibercrime...", p. 722.

tendo inclusive, em matéria de buscas domiciliárias, aparecido, na nossa jurisprudência[195], um caso em que as mesmas foram levadas a cabo dois anos após terem sido decretadas (...) entendemos que, por violação do princípio da actualidade e actualização, tais buscas foram efectuadas de forma ilegítima, já que as razões que presidiram à sua decretação já poderiam não se encontrar presentes à data em que foram levadas a cabo e, ainda, pelo simples facto de que elas poderiam já tornar-se desproporcionadas, desnecessárias e desactualizadas face à evolução da investigação criminal e demais meios de obtenção de prova eventualmente levados a cabo[196]".

Nesse sentido, entende-se que a lacuna deixada pelo legislador nesse artigo pode dar margem a interpretações equivocadas por parte dos magistrados, de extensão indevida de um prazo para aplicação do direito de pesquisa de dados informáticos a um momento que seja oportuno para os órgãos de polícia criminal. Isso só vem a causar ainda mais prejuízo aos direitos fundamentais dos suspeitos ou arguidos.

II- CONCLUSÃO

Com base em tudo o que foi exposto, percebe-se que ao tentar combater os cibercrimes, o legislador português acabou por ocasionar outros problemas, quais sejam a ocorrência de incompatibilizações legislativas entre três diplomas, além do surgimento de normas que ferem os direitos fundamentais das pessoas em prol da recolha e conservação de provas, da busca da verdade e punição dos culpados.

No entanto, esses problemas teriam sido evitados se o legislador tivesse privilegiado a norma geral do CPP em detrimento da criação de novas leis especiais, pois quanto mais legislações existem, maiores as chances de haver incompatibilizações entre elas, bem como lacunas que proporcionam divergências interpretativas e que causam uma insegurança jurídica prejudicial ao combate à cibercriminalidade. No entanto, se for necessário a criação de leis especiais, que o legislador tenha mais cuidado em harmonizá-las, devendo modificá-las quando necessário para que não haja lacunas nem normas incompatíveis entre si que levem a várias interpretações possíveis.

No mesmo sentido, é notório que as normas de obtenção e preservação de prova digital ferem os direitos fundamentais das pessoas e, muito embora esses direitos não sejam

---

[195] Ac. do TRP de 14-02-2007, Processo nº 0617261.

[196] RODRIGUES, Benjamim Silva, "Da prova eletrónico digital...", pp. 525-526.

absolutos, eles requerem a máxima proteção possível, e só podem ser restringidos em casos excecionais, conforme art. 18, nº2, CRP, ou seja, os direitos fundamentais das pessoas só podem ser limitados quando for o único meio necessário de salvaguardar um outro bem jurídico constitucionalmente protegido. Dessa forma, deve haver uma ponderação[197] de interesses com base no princípio da proporcionalidade. Por isso, as normas processuais penais encontradas na lei do cibercrime em causa devem buscar atingir seu fim (combate à cibercriminalidade) com a mínima restrição possível dos direitos fundamentais, que não pode ser abusiva, caso contrário, haveria produção de prova proibida que é nula e não pode ser utilizada, conforme art. 32º, nº8, CRP e 126º, nº3, CPP.

Uma outra solução possível para tentar conciliar o combate à cibercriminalidade (através dos valores eficácia da investigação criminal e tutela da justiça) e a proteção dos direitos fundamentais das pessoas, segundo José Ascensão[198] e Renato Militão[199] seria considerar o direito penal como última *ratio*, ou seja, dar preferência ao ilícito civil, às contra-ordenações puníveis com coimas, o que seria viável já que a maioria dos crimes previstos na lei do cibercrime trazem a possibilidade de punição através de pena de prisão ou pena de multa.

Nesse sentido, é fundamental que o legislador português solucione as incompatibilizações e lacunas legislativas existentes que levam a problemas interpretativos e de segurança jurídica de modo que o combate à cibercriminalidade seja mais eficaz. Também sempre deve ser feita uma ponderação de interesses através do princípio da proporcionalidade de modo que os direitos fundamentais das pessoas sejam protegidos e minimamente afetados em último caso, em prol da busca da verdade, do combate à cibercriminalidade e da realização da justiça.

---

[197] No mesmo sentido, NEVES, Rita Castanheira, *As ingerências nas comunicações*..., pp. 94-95.

[198] ASCENSÃO, José de Oliveira, "O cibercrime...", pp. 316-317, 327.

[199] MILITÃO, Renato Lopes, "*A Propósito da Prova Digital*...", p. 253.

III- BIBLIOGRAFIA

- ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 4ª edição actualizada, 2011.

- ANDRADE, Manuel da Costa, *"Bruscamente no Verão passado"*, *a reforma do Código de Processo Penal,* Coimbra Editora, 2009;

- ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 2013.

- ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2ª edição, 2019.

- ASCENSÃO, José de Oliveira, "O cibercrime" in: *Direito penal económico e financeiro: conferências do curso pós-graduado de aperfeiçoamento,* Coimbra Editora, 2012, pp. 307-327.

- CALVÃO, Clara Guerra e Filipa, *Fórum de Proteção de Dados, Em foco o novo quadro legal europeu, Anotação,* Comissão Nacional de Proteção de Dados, nº1 de julho de 2015, pp. 79-82;

- CANOTILHO, J.J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa anotada*, Vol. I, Coimbra Editora, 1ª edição brasileira, 4ª edição portuguesa revista, 2007;

- CARDOSO, Rui, "Apreensão de correio electrónico e registos de natureza semelhante – artigos 17º da Lei nº 109/2009, de 15.IX"*,* in *Ebook Cibercriminalidade e prova digital*, Centro de Estudos Judiciários, julho 2018;

- CORREIA, João Conde, "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32, nº8, 2ª parte da CRP)?", *Revista do Ministério Público*, nº79 (1999), pp. 45-68;

- CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, nº139 (Julho-Set 2014), pp. 29-59;

- CORREIA, João Conde, "Prova digital: enquadramento legal"*,* in *Ebook Cibercriminalidade e prova digital*, Centro de Estudos Judiciários, julho 2018;

- DIAS, Jorge de Figueiredo; "Revistação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)", *Revista de Legislação e Jurisprudência,* 146 (2016), pp. 3-16.

- MESQUITA, Pulo Dá, "Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime",

in *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer, Coimbra Editora, 2010, pp. 83-129;

- MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal*, 2012, disponível em https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf > consultado em 1-04-19;

- NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova,* Coimbra Editora, 2011.

- NEVES, Rita Castanheira e CORREIA, Hélder Santos; "A Lei do Cibercrime e a colaboração do arguido no acesso aos dados informáticos", *Actualidad Jurídica Uría Menéndez*, nº38, out 2014, pp. 146-149.

- NUNES, Duarte Rodrigues, *Os meios de obtenção de provas previstos na Lei do Cibercrime,* Gestlegal, 2018.

- PINHO, Carlos, "Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações)", *Revista do Ministério Público*, nº 129 (Jan-Mar 2012), pp. 63-93;

- RAMALHO, David/ COIMBRA, José, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *O Direito*, 147, 2015, pp. 997-1045.

- RAMOS, Armando Dias, *A Novíssima Diretiva relativa ao Cibercrime*, 2013, disponível em>https://www.academia.edu/8696174/A_Nov%C3%ADssima_Diretiva_sobre_o_Cibercrime , consultado em 25-04-19.

- RAMOS, Armando Dias, *A prova digital em processo penal: o correio eletrónico*, Chiado editora, 2014;

- RODRIGUES, Benjamim Silva; Da Prova eletrónico digital e da criminalidade informático-digital; *Da Prova Penal*, Tomo IV, Rei dos livros, 2011;

- VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, Coimbra Editora, 2011;

- VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *Revista do Ministério Público,* ano 25, nº 99 (Julho-Set 2004), pp. 117-136.

- VERDELHO, Pedro, "A nova Lei do Cibercrime", *Scientia Iuridica*, Tomo LVIII, nº320, 2009, pp. 717-749;

IV – Outros documentos e links relevantes

- Cibercriminalidade e prova digital, Centro de Estudos Judiciários, julho de 2018, disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Ciber_PDigital2018.pdf > consultado em 4-04-19.

- Comunicado de Imprensa nº 54/14 do Tribunal de Justiça da União Europeia de 8 de abril de 2014, disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/201404/cp140054pt.pdf, consultado em 12-03-19.

- Nota prática nº6/2015, Jurisprudência sobre prova digital, Gabinete do Cibercrime, 27 de agosto de 2015, disponível em <http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_6_jurispridencia_processual.pdf > consultado em 16-03-19.

- Nota prática nº 7/2015; Retenção de dados de tráfego e Lei 32/2008, de 17 de julho; Gabinete do Cibercrime, 30 de dezembro de 2015, disponível em <http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf > acedido a 20-03-19.

- Nota prática nº 8/2016; Pedido de dados a operadores de comunicações, Gabinete do Cibercrime, 18 de fevereiro de 2016, disponível em <http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp.pdf > consultado em 15-04-19.

- Nota prática nº 12/2017, Jurisprudência sobre prova digital, Gabinete do Cibercrime, 2 de novembro de 2017, disponível em <http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_12_jurisprudencia_prova_digital.pdf > acedido a 15-04-19.

- Proposta de Lei nº 289/X/4ª, Exposição de motivos, disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d76574339305a58683062334d76634842734d6a67354c5667755a47396a&fich=ppl289-X.doc&Inline=true > consultado em 12-03-19.

- Relatório Explicativo da Convenção sobre o Cibercrime, STE nº 185, disponível em https://www.cicdr.pt/documents/57891/128776/Convenção+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c > consultado em 12-03-19.

V- JURISPRUDÊNCIA

- Acórdão do Tribunal Constitucional nº 420/2017 de 13-07-17, Processo nº 917/16, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html > consultado em 17-03-19.

- Acórdão do Tribunal da Relação de Évora de 6-01-15, Processo nº 6793/11.2TDLSB-A.E, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument > consultado em 16-03-19.

- Acórdão do Tribunal da Relação de Évora de 20-01-15, Processo nº 648/14.6GCFAR-A.E1, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument > consultado em 16-03-19.

- Acórdão do Tribunal da Relação de Lisboa de 11-01-11, Processo nº 5412/08.9TDLSB-A.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument > consultado em 3-04-19.

- Acórdão do Tribunal da Relação de Lisboa de 19-06-14, Processo nº 1695/09.5PJLSB.L1-9, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_6_jurispridencia_processual.pdf > consultado em 2-04-19.

- Acórdão do Tribunal da Relação de Lisboa de 6-02-18, Processo nº 1950/17.0T9LSB-A.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument > consultado em 3-04-19.

- Acórdão do Tribunal da Relação do Porto de 14-02-07, Processo nº 0617261, disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/6ee9cebc28a61a7f80257284004330de?OpenDocument > consultado em 8-04-19.